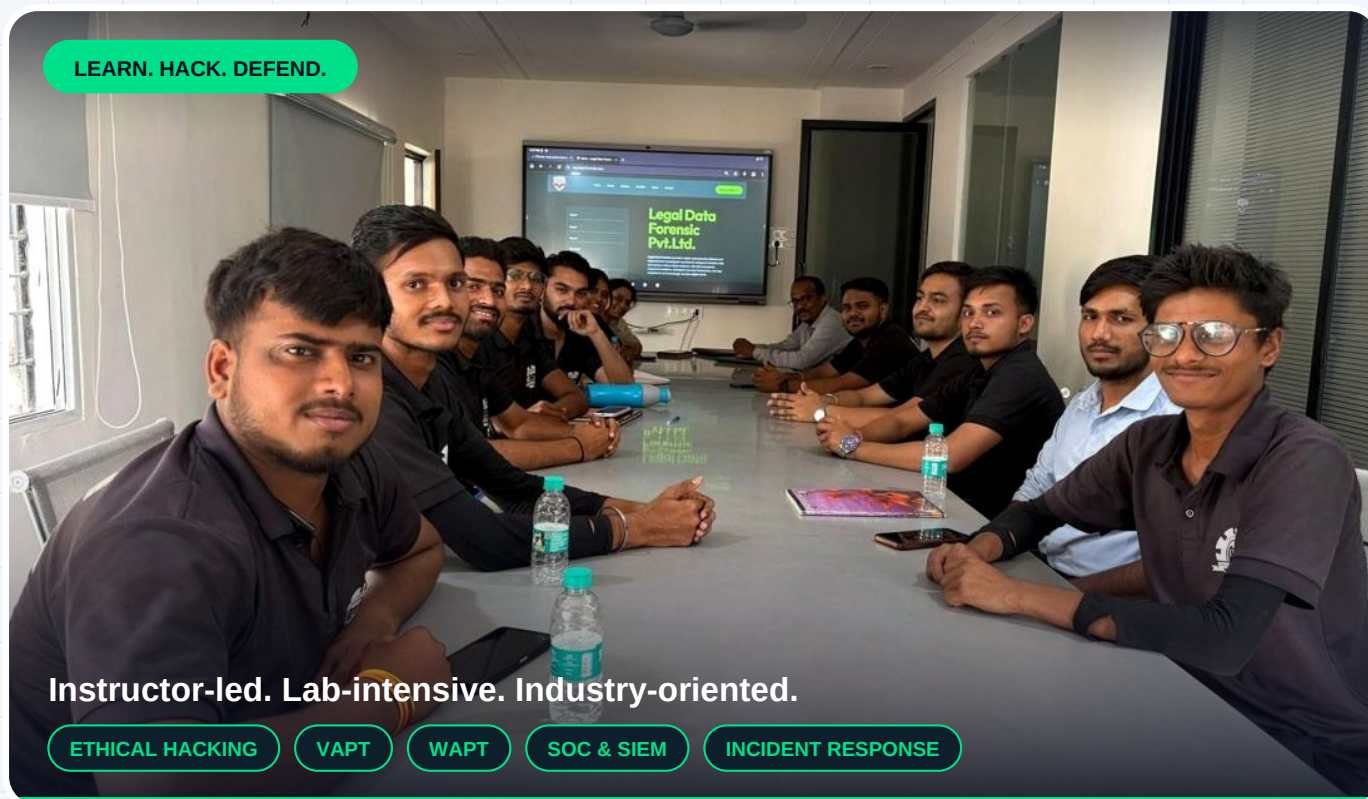




HACKOPS

Ethical Hacking Professional Program

Think Like an Attacker. Work Like a Security Professional.

Master Ethical Hacking. Secure Applications. Detect Threats. Defend Digital Infrastructure.

3

MONTHS

180

TRAINING HOURS

60%

PRACTICAL

9

HANDS-ON LABS

Ethical Hacking | VAPT | WAPT | API Security | SOC & SIEM | Incident Response

upskill.pw

Presented by Crypto Forensic Technology

Proposed course syllabus. Schedule, tools and certification rules are subject to final confirmation by Upskill.

CONTACT US

Phone: 7773900082

Email: shrikant@cryptoforensic.in

Web: www.cryptoforensic.in

Program Overview

A professional, lab-intensive program that joins offensive and defensive security.

HACKOPS is an intensive, practical cybersecurity program covering ethical hacking, Vulnerability Assessment and Penetration Testing (VAPT), Web Application Penetration Testing (WAPT), Security Operations Centre (SOC) operations, incident response and professional security reporting. The curriculum follows common industry workflows reflected in global training programs, including SANS penetration-testing courses, OWASP application-security guidance and professional ethical-hacking curricula, and combines offensive and defensive skills rather than tool demonstrations alone.

Our signature workflow: assess the attack surface, validate security weaknesses, detect suspicious activity, respond to incidents, and communicate findings.

Program at a glance

Program	Details
Program	HACKOPS: Ethical Hacking Professional Program
Duration	3 months / 12 weeks
Training hours	180 hours (suggested)
Delivery	Instructor-led training, guided labs, assignments and projects
Learning approach	30% theory, 60% practical, 10% assessment and review
Level	Foundation to professional
Lab environment	Isolated virtual cyber range and intentionally vulnerable systems
Final outcome	Practical portfolio, assessment reports, SOC investigation and capstone

What you will learn

Ethical Hacking Network penetration testing, recon, scanning and enumeration	VAPT Discovery, validation, CVSS prioritisation and retesting
WAPT and API OWASP Top 10, Burp Suite, REST API security testing	SOC and SIEM Alert triage, log correlation, detection use cases
Threat Detection MITRE ATT&CK mapping, IOCs and threat hunting	Incident Response Evidence preservation, timelines, post-incident reviews
Security Reporting Executive summaries, risk-based remediation advice	Capstone Project Integrated cyber-range assessment and presentation

Detailed 12-Week Syllabus

MONTH 1

Weeks 1-4 | 60 hours

Cybersecurity foundations and ethical hacking

MODULE 1 Cybersecurity and ethical hacking fundamentals

- Cybersecurity landscape, threat actors, attack surfaces and common attack vectors
- CIA triad, security principles, risk, vulnerabilities, threats and exploits
- Ethical hacking lifecycle and penetration-testing methodologies
- Legal authorisation, scope definition, rules of engagement, responsible disclosure
- Overview of PTES, NIST testing guidance and security assessment practices

MODULE 2 Networking, Linux and Windows security

- OSI and TCP/IP models, IP addressing, subnetting, DNS, DHCP, HTTP/S, common ports
- TCP/UDP communication, routing, switching, NAT, VPNs and firewall concepts
- Linux command line, permissions, processes, services, shell scripting, log analysis
- Windows architecture, users, groups, services, event logs and PowerShell basics
- Network traffic analysis using Wireshark

MODULE 3 Reconnaissance, scanning and enumeration

- Passive and active reconnaissance
- OSINT and attack-surface mapping
- DNS, subdomain, service and technology enumeration
- Host discovery and port scanning with Nmap
- Vulnerability scanning concepts and tool-assisted assessment
- Asset discovery, evidence collection and initial risk classification

MODULE 4 Network security and ethical hacking techniques

- Network security controls and common misconfigurations
- Authentication, password security and access-control weaknesses
- Network attack concepts: spoofing, sniffing and session-related risks
- Introduction to Metasploit in controlled lab environments
- Windows and Linux security assessment fundamentals
- Basic vulnerability validation and remediation recommendations

MONTH 1 PRACTICAL OUTCOMES

- ✓ Build a virtual penetration-testing lab
- ✓ Conduct an authorised network discovery exercise
- ✓ Perform a vulnerability scan and validate selected findings
- ✓ Prepare an initial network security assessment report

Detailed 12-Week Syllabus

MONTH 2

Weeks 5-8 | 60 hours

VAPT, WAPT, API and infrastructure security testing

MODULE 5 Vulnerability Assessment and Penetration Testing (VAPT)

- VAPT scope, methodology and engagement planning
- Vulnerability discovery, verification and false-positive analysis
- Prioritisation using CVSS and business impact
- Network and infrastructure penetration-testing workflow
- Exploitation validation and controlled proof-of-concept testing
- Linux and Windows privilege-escalation concepts in labs
- Remediation verification and retesting

MODULE 6 Web Application Penetration Testing (WAPT)

- Web architecture, HTTP requests/responses, cookies, sessions, authentication
- OWASP Top 10 and common web application security risks
- Burp Suite: proxy, repeater, intruder and request analysis
- SQL injection, XSS, CSRF, access-control flaws, security misconfiguration
- File upload flaws, path traversal, SSRF and server-side input validation
- Authentication, authorisation, session management and business-logic testing
- Secure testing practices and evidence-based validation

MODULE 7 API, cloud, wireless and emerging attack surfaces

- REST API security and API testing methodology
- Broken object-level authorisation, excessive data exposure, rate-limit weaknesses
- API authentication, tokens and authorisation controls
- Cloud security: IAM, storage permissions, network exposure, logging
- Wireless security concepts, encryption standards, authorised Wi-Fi assessment
- Mobile application security overview and common mobile risks
- Introduction to container and IoT security assessment

MODULE 8 Penetration-testing reporting and security remediation

- Technical evidence collection and reproducibility
- Severity, likelihood, impact and prioritisation
- Executive summaries and technical findings
- Risk-based remediation and mitigation recommendations
- Retesting and closure validation
- Client communication, confidentiality and professional reporting

MONTH 2 PRACTICAL OUTCOMES

- ✓ Complete a network VAPT exercise
- ✓ Perform a WAPT assessment against an intentionally vulnerable web application
- ✓ Test a sample API for selected security weaknesses
- ✓ Produce a structured VAPT/WAPT report with evidence and remediation guidance

Detailed 12-Week Syllabus

MONTH 3

Weeks 9-12 | 60 hours

SOC operations, incident response and professional capstone

MODULE 9 Security Operations Centre (SOC) fundamentals

- SOC structure, responsibilities, workflows and escalation procedures
- SOC L1 analyst duties and alert triage
- Log sources: endpoints, servers, firewalls, DNS, VPN, applications
- SIEM architecture, event normalisation, correlation and dashboards
- Introduction to Splunk or an equivalent SIEM platform
- Detection rules, use cases, alert severity and prioritisation
- MITRE ATT&CK: mapping observable activity to adversary techniques

MODULE 10 Threat detection and security monitoring

- Security event analysis and log correlation
- Indicators of compromise and threat intelligence fundamentals
- Phishing, suspicious authentication, malware and lateral-movement indicators
- Endpoint detection and response (EDR) concepts
- Network detection and intrusion monitoring
- Basic detection engineering and alert tuning
- Threat hunting fundamentals and investigation documentation

MODULE 11 Incident response and digital investigation

- IR lifecycle: preparation, detection, analysis, containment, eradication, recovery
- Incident classification, severity and escalation
- Initial triage and evidence preservation
- Windows event logs and Linux authentication logs
- Basic forensic acquisition concepts and chain of custody
- Malware incident indicators and ransomware response fundamentals
- Incident timelines, investigation notes and post-incident reviews

MODULE 12 Integrated cyber range and professional capstone

- Simulated enterprise network security assessment
- Controlled red-team versus blue-team exercise
- Vulnerability discovery and attack-path analysis in a lab
- SOC monitoring and investigation of simulated alerts
- Incident handling and response documentation
- Final VAPT report and executive presentation
- Practical evaluation, portfolio review and interview preparation

MONTH 3 PRACTICAL OUTCOMES

- ✓ Investigate a simulated SOC alert
- ✓ Analyse logs and prepare an incident timeline
- ✓ Complete an integrated security assessment and response exercise
- ✓ Present a capstone report and technical findings

Week-wise Training and Practical Schedule

Twelve weeks, each closing with a hands-on assignment.

Wk	Training focus	Key practical assignment
1	Cybersecurity fundamentals, ethical hacking, legal and professional practices	Threat landscape and security assessment worksheet
2	Networking, Linux, Windows and traffic analysis	Network traffic analysis using Wireshark
3	Reconnaissance, OSINT, scanning and enumeration	Authorised network reconnaissance report
4	Network security, vulnerability validation, introductory exploitation	Network vulnerability assessment
5	VAPT methodology, vulnerability scanning and risk assessment	Vulnerability identification and prioritisation
6	Network penetration testing and privilege escalation	Controlled network penetration-testing lab
7	WAPT, OWASP risks and Burp Suite	Web application security assessment
8	API, cloud, wireless security and reporting	API assessment and consolidated VAPT report
9	SOC fundamentals, SIEM and alert triage	SIEM log analysis and alert classification
10	Threat detection, MITRE ATT&CK and threat hunting	Detection use-case and investigation exercise
11	Incident response, evidence preservation, forensic basics	Incident timeline and response report
12	Integrated cyber range, capstone, professional evaluation	Final capstone project and presentation

Industry Tools and Technologies

Offensive security and VAPT	Kali Linux, Nmap, Metasploit Framework, Nessus / OpenVAS
Web and API security	Burp Suite, OWASP resources and testing guides, Postman, OWASP ZAP
SOC and monitoring	Splunk or equivalent SIEM, Wazuh, Wireshark, MITRE ATT&CK
Lab and supporting technologies	VirtualBox / VMware, Docker, Git and GitHub, Python and Bash fundamentals

Tools are indicative. Final selection depends on lab licensing, system requirements, instructor expertise and the availability of equivalent open-source platforms.

Practical Labs and Projects

Nine guided projects that build your portfolio.

Lab / project	Description	Deliverable
Lab 1: Network discovery	Discover hosts, services and exposed ports in a controlled environment	Network map
Lab 2: Vulnerability assessment	Identify and prioritise vulnerabilities on authorised lab assets	Vulnerability assessment report
Lab 3: Network penetration testing	Validate selected weaknesses in an isolated lab	Technical findings and evidence
Lab 4: Web application testing	Assess a vulnerable web application against relevant OWASP risks	WAPT report
Lab 5: API security testing	Test authentication, authorisation and input validation	API security assessment
Lab 6: SOC alert triage	Analyse simulated security alerts using SIEM	Alert investigation record
Lab 7: Threat detection	Map simulated adversary behaviour to MITRE ATT&CK	Detection use-case document
Lab 8: Incident response	Investigate a simulated compromise and preserve evidence	Incident timeline and response report
Capstone	Combine VAPT, SOC monitoring and incident response in a simulated enterprise scenario	Final technical report and presentation

Assessment and Evaluation

Practical lab performance		35%
Assignments and technical reports		20%
Module tests and quizzes		15%
Mid-program practical assessment		10%
Final capstone project		20%

Evaluation checkpoints

- Weekly practical submissions and lab records
- Monthly knowledge and practical assessments
- VAPT and WAPT report-writing evaluation
- SOC investigation and incident-response simulation
- Final capstone demonstration and oral technical review

Completion requirement: at least 75% attendance, completion of mandatory labs and a passing score in the final assessment.

Learning Outcomes

On successful completion, participants should be able to:

- ✓ Explain ethical hacking methodologies and conduct authorised security assessments
- ✓ Identify exposed assets, assess vulnerabilities and validate selected security weaknesses
- ✓ Perform foundational network VAPT and web application security testing
- ✓ Test selected API security controls and understand cloud and wireless security risks
- ✓ Use common security tools to collect, analyse and document technical evidence
- ✓ Triage security alerts and investigate events using SIEM workflows
- ✓ Apply basic incident-response procedures and prepare investigation timelines
- ✓ Produce structured technical reports and communicate risks and remediation recommendations
- ✓ Demonstrate practical skills through a portfolio of lab exercises and a capstone project

Career Pathways

Preparation for entry-level and junior roles.

> Junior Ethical Hacker	> VAPT Analyst
> Junior Penetration Tester	> Web Application Security Tester
> SOC Analyst L1	> Cybersecurity Analyst
> Security Operations Trainee	> Information Security Intern

The program provides foundational and applied preparation for these roles; it does not guarantee employment or independently qualify a participant for every position.

Industry and Certification Alignment

Selected competencies map to the following frameworks.

Framework / program	Relevance to HACKOPS
CompTIA Security+	Security fundamentals, threats, architecture, operations and risk
Certified Ethical Hacker (CEH)	Ethical hacking concepts, reconnaissance, scanning and attack methodologies
OffSec PEN-200 / OSCP	Practical penetration-testing workflow, enumeration, exploitation and reporting
OWASP Web Security Testing Guide	Web application testing methodology and vulnerability coverage
MITRE ATT&CK	Threat detection, investigation and adversary behaviour mapping
NIST SP 800-115	Security testing and assessment processes
NIST SP 800-61	Incident-response processes and operational readiness

These are alignment references, not claims of accreditation, official certification partnership or full exam coverage. Certification preparation can be offered as an additional component.

Ready to go beyond the theory?

Build practical cybersecurity skills.
Develop your technical portfolio.
Prepare for your next step in cybersecurity.

Enrol at upskill.pw

Explore the full program, batches and fees at <https://upskill.pw/>

CONTACT US

PHONE **7773900082**
EMAIL **shrikant@cryptoforensic.in**
WEB **www.cryptoforensic.in**



Crypto Forensic Technology

HACKOPS is a lab-based training program. It does not guarantee employment, accreditation, or exam coverage of any third-party certification.
All offensive techniques are practised only in isolated, authorised lab environments.