6-Month "**Real-World Diploma**" in

Offensive Security & Digital Forensics

From classroom to cyber-war-room in 180 days

Goal : *Turn yourself from graduate-in-waiting to breach-hunter, cyber-sleuth and instant hire.*

Why this diploma, why now?

India will need **1.5 million cyber-security specialists by 2028** (NASSCOM). Yet most fresh engineers graduate knowing TCP/IP theory but not how to **detect, disrupt and dissect** real-world attacks. This programme fast-tracks you through exactly those battlefield skills—and backs them with an employability guarantee.

What you'll master in just 180 days?

Phase	Real-world skill you'll own
Security Basics	Use OSINT, Shodan and Metasploit to breach a live enterprise in a legal range.
Cybersecurity Foundations	Build attack labs, exploit common misconfigurations, use Metasploit, and secure environments with defensive security tooling.
Offensive Security	Breach targets with OSINT, Burp Suite & Metasploit, exploit web vulnerabilities (SQLi, XSS, SSRF, RCE), escalate privileges, and simulate real-world Red Team attacks.
Defensive Security	Detect and hunt threats using SIEM (Splunk/ELK), perform memory forensics with Volatility, investigate breaches, and respond like a SOC analyst with IR playbooks.

72-hr Purple-Team Hackathon	Team up with classmates to defend a company network against pro red-teamers—winner pockets real bug-bounty cash.

Output Portfolio: 3 exploit videos, 2 blue-team playbooks, 1 court-ready forensic report + your mock-testimony reel—deliverables recruiters can't ignore.

How we deliver mastery?

- **Cyber-Range Campus** – Each learner gets a 40-node cloud lab (resets in 90 seconds) to break and defend daily.
- **Mentors, not lecturers** – Direct 1:4 guidance from industry-certified experts (CEH, CySA+) and ex-CERT professionals with global consulting experience.
- **Edge-Tech Toolkit** – Kali, Metasploit, Burp Suite Pro, Splunk, Autopsy, Volatility—all included.
- **Legal s Ethics Track** – Co-taught by a cyber-crime prosecutor so you know how to keep hacks ethical and evidence admissible.

Placement s Career Lift

Metric	Guarantee
Placement window	Job-ready within **60 days** of graduation or we keep reskilling you free.
Average starting CTC	2.5× your current internship stipend
Recruiter pool	Big-4 DFIR teams, CERT-In empanelled SOCs, global MSSPs, bug-bounty platforms.

Plus, you keep earning: 10 % of any bug-bounty payouts during the programme go straight into your pocket.

Who should apply?

Final-year B.E./B.Tech/BSc (CS, IT, ECE) students who:

1. Can write basic Python or C and aren't afraid of a Linux terminal.
2. Crave real hacking—not just multiple-choice certs.
3. Want a career where every day is a high-stakes puzzle (and pays like it).

Ready to swap capstone mini-projects for real incident-response creds? Seats are limited to keep mentor ratios tight—apply by **<date>** at **isparklearning.com/cyber-diploma** and book a 20-minute CTF challenge to secure your spot.

---

1. Programme North Star

Element	Description
Purpose	Produce *elite first-responder technologists* who can detect, disrupt and debrief advanced cyber-attacks within *15 minutes*, and who can stand up in court to defend their forensic chain-of-custody.
Graduate Promise	• Tier-1 SOC / CERT job offer or funded bug-bounty retainer within 60 days of graduation. • Portfolio: 3 red-team exploits, 2 blue-team playbooks, 1 admissible forensic report C expert-witness mock testimony video.

Element	Description
Mindset Shifts	"From student to threat-hunter" • "Evidence > opinion" • "Assume breach; respond in minutes, not months."

2. Curricular Scaffold (26 Weeks, ~650 Hours)

Phase	Duration	Immersive Sprint	Real-World Artefact
0. Boot-Camp	1 wk	Introduction to Cybersecurity, Network Fundamentals, How the Web Works, Linux & Windows Fundamentals, Command Line & Scripting Basics	Personal war-room VM image
1. Cybersecurity Foundations	3 wks	AD Fundamentals, Cryptography Basics, Exploitation Basics, Metasploit Framework, Web Hacking Fundamentals, Security Solutions, Defensive Security Tooling	Foundation Lab Completion Badge
2. Pentesting	4 wks	Reconnaissance & Enumeration, Vulnerability Discovery, Privilege Escalation (Windows/Linux), Burp Suite Deep Dive, Network Exploitation	Red Team Playbook #1

3. Web Application Pentesting	3 wks	Authentication & Authorization Bypass, SQL Injection, Command Injection, File Inclusion, Advanced Server-Side Attacks (SSRF, RCE), Advanced Client-Side Attacks (XSS, CSRF, Request Smuggling)	*Bug Bounty Exposure*
4. CompTIA Pentest+	4 wks	Engagement Management, Reconnaissance & Enumeration, Vulnerability Discovery & Analysis, Attacks & Exploits, Post-Exploitation & Lateral Movement	*Pentest+ Report + Exploit Demonstration*
5. SOC & Digital Forensics	4 wks	Cyber Defence Frameworks (NIST, MITRE ATT&CK), Threat Intelligence, Traffic Analysis, Endpoint Security Monitoring, SIEM (Elastic/Splunk), Digital Forensics (Autopsy, Volatility), Incident Response	*Forensic Case Report + SOC Dashboard*

6. CompTIA CySA+	4 wks	Security Operations, Vulnerability Management, Threat Hunting, Incident Response, Reporting & Communication	*CySA+ Threat Detection Report*
7. Capstone: Purple-Team Fusion Day	1 wk (72-hr hack)	3-person crews defend live cyber-range vs. pro red-teamers (prize money bounty)	Executive after-action debrief (CISO audience)
8. Career Accelerator	2 wks	CV reverse-engineering, LinkedIn teardown, mock HR C technical interviews, CPRG-style bug-bounty challenge	Offer-letter scoreboard

3. Experiential Delivery Stack

Layer	Implementation
Cyber-Range-as-Campus	Cloud-native range (OpenStack + Terraform) spins 40-node enterprise network per learner; auto-resets in 90 s.
Evidence-Locker Chain	Private IPFS ledger stamps every forensic artefact; hashes exposed to guest magistrate for authenticity drills.
Immersive Clinics	Every Friday: "Breach-of-the-Week" led by invited DFIR leads from Apple, CBI, or Singapore CSA.

1:4 Mentor Ratio	Pool of OSCP, SANS 508/560, ex-CERT officers. *No lecture > 30 mins*; 70 % of time in guided missions.
Ethics s Legal Track	Co-taught with practising cyber-crime prosecutor; mandatory module on personal liability C data-privacy laws (GDPR, PDPB-India).

4. Tool-Chain s Certifications Mapped

Domain	Primary Tools	Optional Global Cert Alignment
Offensive Security	Kali Linux, Burp Suite Pro, Nmap, Metasploit, Cobalt Strike, Hydra, SQLMap, wfuzz, BeEF	CompTIA Pentest+, CEH, eJPT, PT1
Defensive Security	Elastic Stack (ELK), Splunk, Suricata, Zeek, Security Onion, Autopsy, Volatility, Magnet AXIOM, FTK Imager	CompTIA CySA+, SAL1, CHFI, Splunk Core Certified

(*Exam vouchers subsidised 50 % for top-quartile performers*)

5. Admission s Assessment

- **Intake:** final-year BTech / BSc (CS, IT, ECE) or working pros ≤ 3 yrs exp.
- **Admission test:** 90-min CTF + evidence-integrity caselet.
- **Grading:** 40 % live-range performance, 25 % artefact quality, 20 % peer review, 15 % ethics compliance.
- **Fail-fast Policy:** two consecutive "breach-fail" flags → mandatory tutoring or exit with micro-credential.

6. Industrys Government Partnerships

Partner	Contribution	Student Benefit
Palo Alto Networks	100 firewall VM licences C threat-intel feeds	Real-time IOC ingestion
Indian Computer Emergency Response Team (CERT-In)	Monthly threat briefings; guest incident escalation	Authentic nation-scale scenarios
Big 4 DFIR units	Capstone adjudicators; direct hiring pool	Fast-track interview slots
Bugcrowd / HackerOne	Sponsored bounty challenges	Cash earnings before graduation

7. Outcome Metrics

KPI Target	Year 1 Cohort
Graduation rate	≥ 85 %
First-offer placement	≥ 90 % <60 days

KPI Target	Year 1 Cohort
Average CTC uplift	2.5X pre-programme
Employer NPS (first 6 mo)	≥ 75