EDVANTA

Ignite your growth, inspire your mind

ONLINE COURSE

Cybersecurity & Ethical Hacking

From Foundations to Field-Ready

A practical, industry-aligned 12-week program designed for early professionals, graduate students, and career changers. Build real skills, work with real tools, and step into the cybersecurity workforce with confidence.

12 Weeks Structured, phase-based learning	**3 Phases** Foundation → Intermediate → Advanced
Live Mentoring Weekly 1:1 and small-group sessions	**Job-Ready** Aligned to current industry roles

EDVANTA

EDVANTA

Ignite your growth, inspire your mind

Why This Course Matters Today

Cybersecurity is no longer a niche — it is a boardroom priority. Organizations worldwide face a critical skills shortage just as threats escalate in frequency and sophistication. This course bridges the gap between academic theory and what employers actually need on day one.

Escalating Threat Landscape

Ransomware, supply-chain attacks, and zero-day exploits are at an all-time high. Organizations need defenders who understand attacker methodology, not just compliance checklists.

Global Talent Shortage

Over 3.5 million cybersecurity positions remain unfilled globally. Employers are actively hiring early-career professionals who demonstrate hands-on, practical skills.

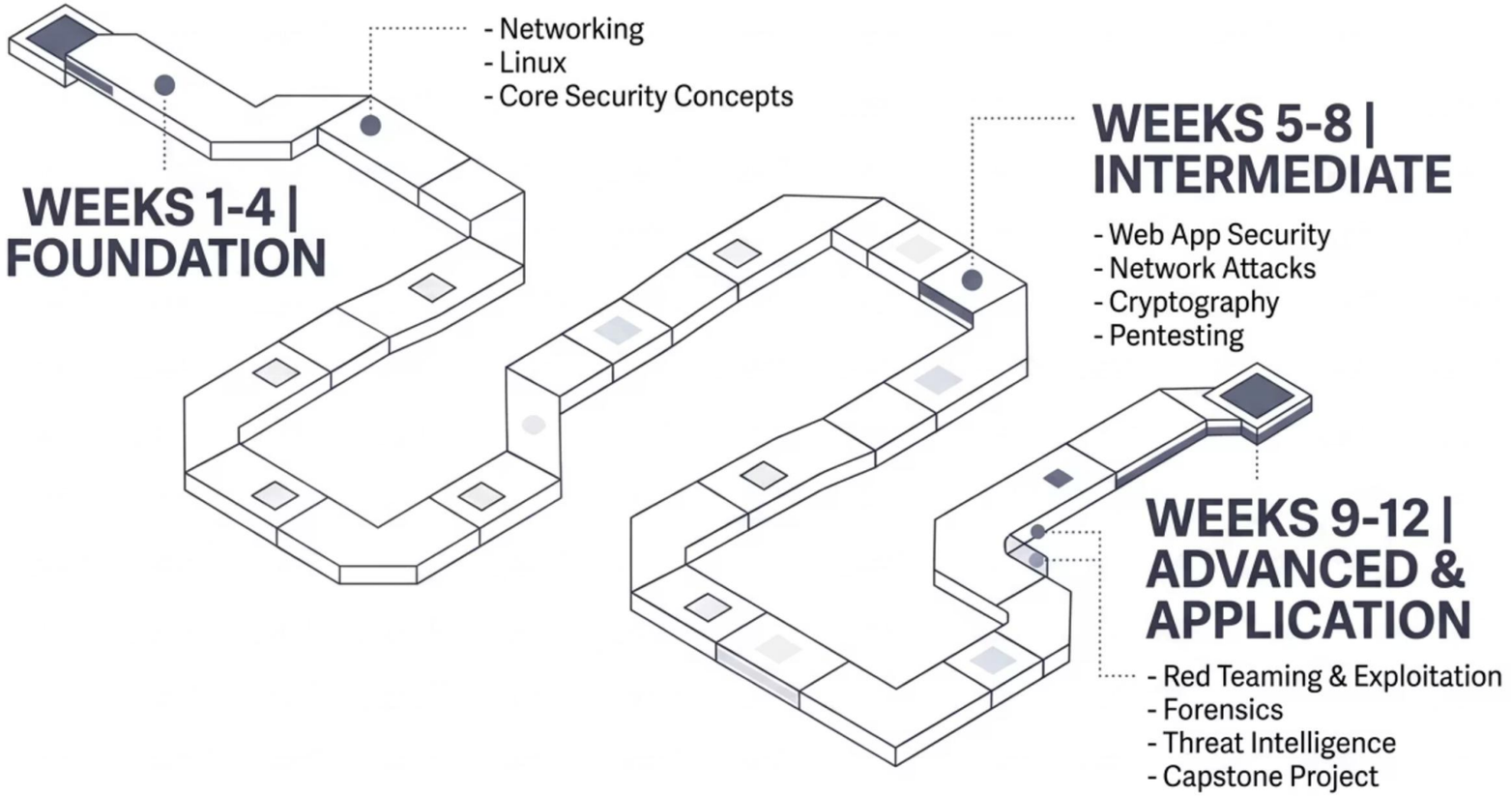
High-Growth Career Path

Cybersecurity roles consistently rank among the fastest-growing and highest-paying in tech. Ethical hackers and security analysts command premium salaries across every industry vertical.

EDVANTA

Course Architecture at a Glance

The program is divided into three progressive phases. Each phase builds deliberately on the last — ensuring you develop the deep fundamentals required to handle advanced topics with confidence.



Weekly Format

- Weekend recorded concept session (90 min)
- Weekend live mentoring session (60 min)
- Hands-on lab or practical exercise
- Weekly assignment or mini project

Content Balance

- 70–80% core concepts and fundamentals
- 10–15% industry use cases and real scenarios
- Remaining time: tool demos and workflows
- All phases include a capstone deliverable

EDVANTA

Ignite your growth, inspire your mind

PHASE 1 — WEEKS 1–4

Foundation Phase

The first four weeks establish the technical bedrock every cybersecurity professional must have. You will build fluency in networking, Linux, core security principles, and begin using essential reconnaissance tools — skills that underpin every advanced topic ahead.

1

Week 1: Networking & Protocols

- OSI and TCP/IP models — layer-by-layer breakdown
- DNS, DHCP, HTTP/S, FTP, SSH protocol deep dives
- Subnetting, CIDR notation, and IP addressing
- Packet capture fundamentals with Wireshark
- Network topologies and common infrastructure patterns
- Lab: Analyze live traffic and identify protocol anomalies

2

Week 2: Linux for Security

- Linux filesystem hierarchy and permissions model
- Essential CLI commands for security workflows
- Bash scripting basics for task automation
- User management, sudo, and privilege concepts
- Log files: where they live and what they reveal
- Lab: Build and navigate a Kali Linux environment

3

Week 3: Core Security Concepts

- CIA Triad: Confidentiality, Integrity, Availability
- Authentication, authorization, and access control models
- Threat actors, attack surfaces, and threat modeling
- Security policies, standards, and compliance basics
- Introduction to MITRE ATT&CK framework
- Lab: Perform a basic threat model on a sample application

4

Week 4: Reconnaissance & OSINT

- Passive vs. active reconnaissance — when and how
- OSINT techniques: Shodan, Google dorks, WHOIS
- DNS enumeration and subdomain discovery
- Maltego for relationship mapping and visualization
- Footprinting methodology and professional reporting
- Mini Project: Full OSINT profile on a target organization

EDVANTA

EDVANTA

Ignite your growth, inspire your mind

PHASE 2 — WEEKS 5–8

Intermediate Phase

With a solid foundation in place, weeks 5–8 move into active offensive and defensive techniques. You will perform your first real penetration tests, exploit web vulnerabilities, break and build cryptographic understanding, and begin thinking like both attacker and defender simultaneously.

1

Week 5: Scanning & Enumeration

- Host discovery and port scanning with Nmap
- Service version detection and OS fingerprinting
- Vulnerability scanning with Nessus and OpenVAS
- Banner grabbing and manual service enumeration
- SMB, SNMP, and LDAP enumeration techniques
- Lab: Full scan and enumeration report on a test network

2

Week 6: Web Application Security

- OWASP Top 10 — understanding and exploiting each
- SQL injection: manual and automated with SQLMap
- Cross-Site Scripting (XSS) and CSRF attacks
- Authentication bypass and broken access control
- Burp Suite: intercepting, modifying, and replaying requests
- Lab: Attack a deliberately vulnerable app (DVWA/WebGoat)

3

Week 7: Network Attacks & Defense

- ARP spoofing and Man-in-the-Middle attack chains
- Password attacks: brute force, dictionary, rainbow tables
- Sniffing and session hijacking concepts
- Firewall evasion and IDS/IPS bypass techniques
- Defensive countermeasures and network hardening
- Lab: Execute and detect a MitM attack in a lab environment

4

Week 8: Cryptography & Pen Test Methodology

- Symmetric vs. asymmetric encryption — practical distinctions
- PKI, digital signatures, certificates, and TLS/SSL
- Hashing algorithms and password cracking with Hashcat
- Penetration testing phases: plan, recon, scan, exploit, report
- Scope, rules of engagement, and legal authorization
- Mini Project: End-to-end pen test on a vulnerable VM

EDVANTA

EDVANTA

Ignite your growth, inspire your mind

PHASE 3 — WEEKS 9–12

Advanced & Application Phase

The final four weeks place you in scenarios that mirror real professional engagements. Topics include advanced exploitation, red team operations, digital forensics, and threat intelligence — culminating in a capstone project that demonstrates job-ready competence.

1

Week 9: Exploitation & Post-Exploitation

- Metasploit Framework — modules, payloads, and sessions
- Privilege escalation on Windows and Linux targets
- Maintaining access: persistence mechanisms and backdoors
- Lateral movement concepts and pivoting techniques
- Covering tracks and anti-forensics basics
- Lab: Full exploitation chain on a multi-service target VM

2

Week 10: Red Teaming & Social Engineering

- Red team vs. blue team vs. purple team distinctions
- Social engineering: phishing, vishing, and pretexting
- Physical security testing concepts and tailgating scenarios
- Command-and-control (C2) framework overview
- Adversary simulation with frameworks like Cobalt Strike (demo)
- Lab: Craft a targeted phishing simulation and analyze results

3

Week 11: Digital Forensics & Incident Response

- DFIR lifecycle: preparation, identification, containment, eradication
- Evidence collection, chain of custody, and legal considerations
- Disk and memory forensics with Autopsy and Volatility
- Log analysis and timeline reconstruction
- Threat intelligence: IOCs, threat feeds, and MISP
- Lab: Investigate a simulated breach and write an IR report

4

Week 12: Capstone Project & Career Prep

- Full-scope penetration test on a multi-service lab environment
- Professional pentest report writing — executive and technical sections
- Portfolio building: GitHub, write-ups, and CTF contributions
- Mock interview preparation and resume review
- Certification roadmap: CEH, OSCP, CompTIA Security+
- Final Deliverable: Capstone report and live demo presentation

EDVANTA

Tools & Technology Stack

Proficiency with industry-standard tools is a non-negotiable hiring criterion. This course builds hands-on competency across the full professional toolkit — organized by function so you always know which tool to reach for in the field.

Reconnaissance

- Maltego
- Shodan
- theHarvester
- Recon-ng
- WHOIS / DNSdumpster

Scanning & Enumeration

- Nmap / Zenmap
- Nessus
- OpenVAS
- Nikto
- Gobuster / Dirb

Exploitation

- Metasploit Framework
- SQLMap
- Burp Suite
- Hydra / John the Ripper
- ExploitDB / Searchsploit

Forensics & Defense

- Autopsy
- Volatility
- Wireshark
- Splunk (SIEM)
- MISP (Threat Intel)

Environments

- Kali Linux
- Parrot OS
- TryHackMe
- HackTheBox
- VulnHub / DVWA

Industry Example 1: Ransomware Attack on a Healthcare Provider

The Business Problem

A regional hospital network was hit by a ransomware variant that encrypted patient records and demanded a $4M ransom. Backup systems were also compromised, creating a full operational crisis affecting patient care.

Role of Early Professionals

Junior security analysts triaged alerts, isolated infected endpoints, supported forensic image collection, and documented the breach timeline under senior supervision — critical real-world exposure.

How Course Concepts Applied

- **Week 11 DFIR skills** guided the evidence collection and chain-of-custody process
- **Network traffic analysis** (Wireshark) revealed the lateral movement path
- **Threat intelligence** identified the ransomware family via MISP feeds
- **Log analysis** in Splunk reconstructed the attacker timeline

Measurable Business Impact

- Containment achieved within 6 hours of detection
- Clean backup restoration completed in 48 hours
- Ransom not paid — estimated $4M saved
- IR report used to redesign backup architecture

Tools Used: Splunk, Wireshark, Autopsy, Volatility, MISP — all covered directly in this course's Phase 3 curriculum.

Industry Example 2: Web App Pen Test for a Fintech Startup

The Business Problem

A fintech startup preparing for SOC 2 Type II certification hired an external pen testing firm to assess their customer-facing payment portal before a regulatory audit. The security of user financial data was directly at stake.

How Course Concepts Applied

- **OWASP Top 10 methodology** (Week 6) structured the entire test plan
- **Burp Suite** was used to intercept and manipulate payment API requests
- **SQL injection testing** revealed an exploitable parameter in the login flow
- **Broken access control** allowed one user to view another's transaction history

Measurable Business Impact

- 3 critical and 7 high-severity findings documented
- All critical vulnerabilities patched before the SOC 2 audit
- Startup passed certification — unlocking enterprise client contracts
- Pen test report became the foundation of their security roadmap

Role of Early Professionals

Junior testers executed reconnaissance, performed automated scans, manually validated findings, and contributed to the professional report — exactly the workflow this course replicates in labs.

Tools Used: Burp Suite, SQLMap, Nmap, OWASP ZAP — all hands-on tools covered in Phase 2 of this program.

Industry Example 3: Insider Threat Detection at an Enterprise Bank

The Business Problem

A major bank's Security Operations Center detected unusual data exfiltration activity on their SIEM platform. An internal employee was found systematically downloading customer PII to a personal cloud storage account over three weeks.

Role of Early Professionals

SOC analysts at Tier 1 and Tier 2 identified anomalous behavior through alert triage, escalated to the DFIR team, assisted in evidence preservation, and produced the initial incident report for legal review.

How Course Concepts Applied

- **SIEM log analysis** (Splunk, Week 11) surfaced the exfiltration pattern
- **User behavior baselines** and anomaly detection from core security concepts
- **Chain of custody procedures** ensured evidence was court-admissible
- **Threat modeling** (Week 3) informed the internal access control review

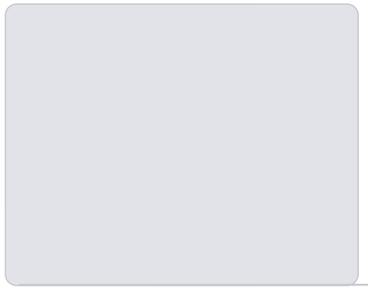
Measurable Business Impact

- Exfiltration stopped before data was publicly exposed
- Legal action pursued successfully using preserved forensic evidence
- Bank avoided an estimated $12M regulatory fine
- DLP policy and monitoring revamped enterprise-wide

Tools Used: Splunk SIEM, Autopsy, Volatility, internal DLP platform — reinforcing the direct link between course skills and SOC-level work.

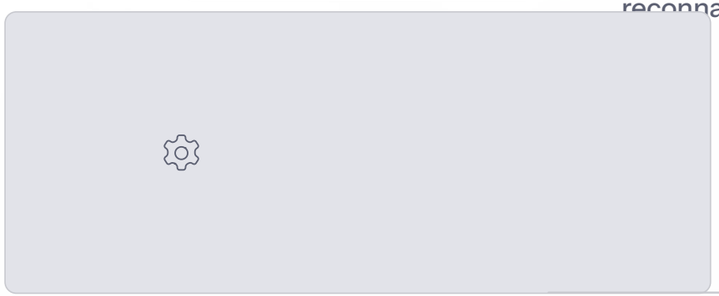
Skills Progression Map

This course is intentionally designed as a three-stage skills ladder. Each milestone builds on the last, moving you from conceptual understanding to genuine job-readiness. Track your progress and know exactly where you stand at every phase.



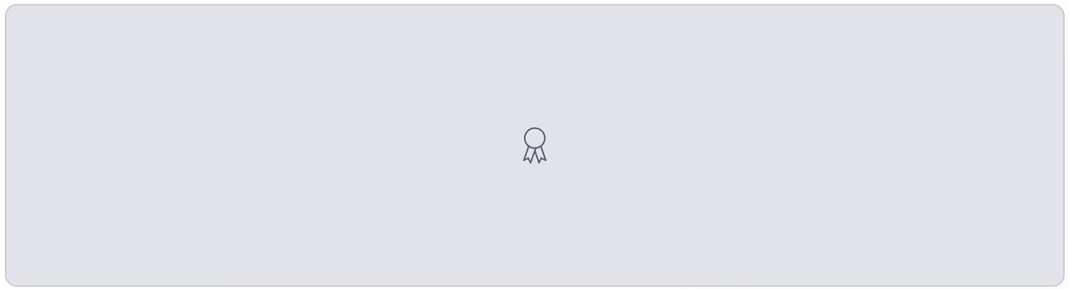
Beginner (Weeks 1–4)

- Understands OSI/TCP-IP, DNS, and basic networking
- Comfortable in a Linux CLI environment
- Knows core security concepts and threat modeling
- Can perform basic OSINT and passive reconnaissance



Intermediate (Weeks 5–8)

- Runs Nmap scans and interprets vulnerability reports
- Exploits OWASP Top 10 vulnerabilities with Burp Suite
- Performs network-level attacks in controlled environments
- Executes and documents a structured penetration test



Job-Ready (Weeks 9–12)

- Full exploitation chains using Metasploit with post-exploitation
- Conducts red team simulations and social engineering campaigns
- Investigates incidents and writes professional DFIR reports
- Delivers a polished capstone penetration test with executive summary

Career Alignment: Job Roles This Course Prepares You For

Completing this program positions you for entry-level to junior roles across the most in-demand areas of the cybersecurity job market. Each role maps directly to skills built throughout the 12 weeks.

SOC Analyst (Tier 1 & 2)

Monitor security events, triage alerts, and escalate incidents. Directly leverages Splunk, Wireshark, and log analysis skills from Weeks 7 and 11. The most common entry point into cybersecurity.

Junior Penetration Tester

Perform authorized vulnerability assessments and pen tests on web apps and networks. Requires Burp Suite, Metasploit, and report-writing competencies built across Phases 2 and 3.

Vulnerability Analyst

Scan and assess systems for vulnerabilities, prioritize remediation, and track risk. Nessus, OpenVAS, and CVSS scoring knowledge from Week 5 are core daily-use skills.

Digital Forensics Analyst

Investigate security incidents, collect and analyze evidence, and support legal proceedings. Autopsy, Volatility, and chain-of-custody training from Week 11 are directly transferable.

Threat Intelligence Analyst

Research threat actors, analyze IOCs, and produce intelligence reports. MISP, MITRE ATT&CK framework knowledge, and OSINT skills from Weeks 4 and 11 underpin this role.

Security Engineer (Entry)

Implement and maintain security controls, firewalls, and monitoring systems. Foundation networking, access control, and hardening concepts from Weeks 1–3 and 7 provide the required groundwork.

EDVANTA

Ignite your growth, inspire your mind

Your Post-Course Roadmap

Completing this program is a launchpad, not a finish line. Here is the recommended path forward to accelerate your career in the 6–18 months following graduation.

1 Month 1–2 Post-Course

- Sit for **CompTIA Security+** certification — validates your foundations to employers
- Publish your capstone report on GitHub as a portfolio piece
- Register on TryHackMe and HackTheBox — solve 2–3 machines per week

2 Month 3–6 Post-Course

- Target your first role: SOC Analyst, Junior Pen Tester, or Vulnerability Analyst
- Begin **CEH (Certified Ethical Hacker)** or **eJPT** (eLearnSecurity Junior Pen Tester)
- Participate in Capture the Flag (CTF) competitions — document write-ups publicly

3 Month 6–12 Post-Course

- Work toward **OSCP (Offensive Security Certified Professional)** — the gold standard
- Specialize: Red Teaming, Cloud Security, or Malware Analysis tracks
- Build a professional network through DEFCON, BSides, and OWASP chapters

4 12–18 Months Post-Course

- Pursue mid-level certifications: **PNPT, GPEN, or GWAPT**
- Contribute to open-source security tools or bug bounty programs (HackerOne, Bugcrowd)
- Mentor incoming learners — teaching accelerates mastery and builds credibility

EDVANTA

EDVANTA

Ignite your growth, inspire your mind

Key Takeaways

Before you begin Week 1, internalize these principles. They define not just how this course is structured, but how exceptional cybersecurity professionals approach their craft every single day.

Think Like an Attacker to Defend Like a Pro

The best defenders understand offensive techniques firsthand. Ethical hacking teaches you to see systems through an attacker's eyes — enabling you to anticipate, detect, and neutralize threats before they escalate.

Fundamentals Are Your Force Multiplier

Networking, Linux, and core security concepts are not prerequisites to skip through — they are the foundation every advanced skill is built on. Master them deeply and everything else accelerates.

Tools Don't Make the Professional — Judgment Does

Nmap, Metasploit, and Burp Suite are only as effective as the person running them. This course trains your analytical thinking, not just your button-clicking. Employers hire for both.

Documentation Is Half the Job

A brilliant pen test with a poorly written report delivers zero business value. Every week, you practice translating technical findings into clear, actionable language for technical and non-technical stakeholders alike.

Ethics and Legality Are Non-Negotiable

Every technique in this course is taught within strict legal and ethical boundaries. Understanding scope, authorization, and responsible disclosure is what separates a security professional from a criminal actor.

EDVANTA

EDVANTA

Ignite your growth, inspire your mind

Ready to Build Your Cybersecurity Career?

Twelve weeks. Three phases. One goal: transforming you from a curious learner into a confident, job-ready security professional. The threats are real, the demand is urgent, and the opportunity has never been greater. Your journey starts now.

12

Weeks of Structured Learning

Progressive, phase-based curriculum designed for working learners

50+

Hands-On Labs & Exercises

Real tools, real environments, real scenarios every week

3.5M

Open Cybersecurity Jobs Globally

The talent gap you are stepping into is massive and urgent

6

Target Career Roles

SOC Analyst, Pen Tester, Forensics, Threat Intel, and more

Next Step: Review your Week 1 pre-reads, set up your Kali Linux lab environment, and join the course community channel. Your first live mentoring session is scheduled for the end of Week 1 — come with questions.

EDVANTA