Transf tech
ACADEMY

AI-Powered
Cybersecurity Engineering
Offensive Security

40	100%	95%
CLASSES	HANDS-ON	JOB READY

Program Summary

This program develops elite offensive security professionals capable of operating in AI-augmented threat environments. Built around a >90% hands-on lab delivery model across **40 classes**, every theoretical concept is immediately reinforced through practical exploitation, analysis, and reporting in real-world-equivalent lab environments. Graduates are equipped to pursue high-value cybersecurity roles in the USA and international markets — including AI Red Team Operator, Offensive Security Engineer, and Vulnerability Researcher — with estimated 2026 starting salaries ranging from **$90,000** to **$345,000**.

Graduate Employability Outcomes

- AI Red Team Operator
- Penetration Tester
- Malware Analyst
- Vulnerability Researcher
- AppSec Engineer (AI-Focus)
- Technical Security Auditor
- Threat Intelligence Analyst
- Offensive Security Engineer

Program Structure

1	Foundations	C1-4
2	Secure Lab Setup	C5-8
3	Cyber Intelligence	C8- 10
4	PentestOps	C11-27
5	Hardening	C28-31
6	AI Security	C32- 33
7	Cloud Security	C34-35
8	AI Sec Ops	C36-37
9	GRC	C38
10	CareerOps	C39-40

40 Classes

80 Hours Live + Guided Lab Sessions

PHASE 1: Information Security Foundations & Risk Intelligence

Classes 1–4

1 Information Security Fundamentals

Class 1–2

Core Activities

- CIA Triad: Confidentiality, Integrity, Availability
- Modern Threat Landscape: Malware, Phishing, Ransomware, APTs, Social Engineering
- Cybersecurity Career Pathways: Penetration Tester, AI Red Teamer, Malware Analyst, Threat Intelligence Analyst
- Real-World Breach Case Studies: Business & Operational Impact Analysis
- Ethics & Legal Boundaries of Offensive Security
- Introduction to Offensive Security Mindset

Labs & Tools

- Scenario-Based Discussion (In-Class)
- ChatGPT / Claude / Gemini — AI Security Assistants
- TryHackMe — Introduction to Cybersecurity Room

1 Risk Assessment — Techniques, Frameworks & Risk Register

Class 3–4

Core Activities

- Risk Assessment Techniques: Qualitative, Quantitative, Semi Quantitative
- Risk Identification, Likelihood-Impact Scoring & Risk Appetite
- Treatment Strategies: Accept / Mitigate / Transfer / Avoid
- Formal Risk Register Preparation: Risk Owners, Severity Ratings, Timelines, Remediation Actions
- OWASP Risk Rating Methodology

Labs & Tools

- Practical Risk Register Exercise (In-Class Demonstration)
- NIST CSF 2.0 Framework Reference
- OWASP Risk Rating Calculator
- Claude / ChatGPT — DREAD/CVSS Scoring Assistance

PHASE 2: Lab Engineering & Linux Offensive Foundations
Classes 5–7

2 Kali Linux Installation & Environment Configuration
Class 5

Core Activities

- Kali Linux Deployment in VirtualBox / VMware
- Network Isolation Configuration: NAT, Host-Only, Bridged
- VM Snapshot Management & Lab Environment Best Practices
- Pre Installed Offensive Tool Categories: Inventory & Classification
- Legal & Ethical Boundaries of Offensive Security Tool Use

Labs & Tools

- VirtualBox / VMware Workstation Player
- Kali Linux (Latest Release)
- ChatGPT / Claude — Hypervisor Error Troubleshooting

2 Linux Troubleshooting & Problem Solving
Class 6

Core Activities

- Diagnosing Common Kali Linux Issues: Package Conflicts, Vmware/Virtualbox issues, Driver Failures, Network Misconfigurations, Permission Errors & apt Error Output Interpretation

Labs & Tools

- Kali Linux Terminal — Break-Fix Lab Scenarios
- Claude / ChatGPT — Real Time Linux Troubleshooting Co-Pilot

PHASE 2: Lab Engineering & Linux Offensive Foundations

Classes 5–7

2 Linux Commands & Bash Scripting for Offensive Security

Class 7

Core Activities

- Core Terminal Commands: ls, cd, chmod, chown, grep, awk, sed, netstat, ps, curl, wget
- Bash Scripting for Offensive Task Automation
- Port Scanning Automation
- OverTheWire Bandit Wargame Challenges
- Shell Scripting Best Practices for Security Professionals

Labs & Tools

- Kali Linux Terminal & Bash Shell
- OverTheWire: Bandit Wargame
- ChatGPT / Claude — Bash Script Generation & Debugging

PHASE 2: Lab Engineering & Linux Offensive Foundations

Classes 5–7

2 Linux Commands & Bash Scripting for Offensive Security

Class 7

Core Activities

- Core Terminal Commands: ls, cd, chmod, chown, grep, awk, sed, netstat, ps, curl, wget
- Bash Scripting for Offensive Task Automation
- Port Scanning Automation
- OverTheWire Bandit Wargame Challenges
- Shell Scripting Best Practices for Security Professionals

Labs & Tools

- Kali Linux Terminal & Bash Shell
- OverTheWire: Bandit Wargame
- ChatGPT / Claude — Bash Script Generation & Debugging

PHASE 3: Threat Intelligence, OSINT & Social Engineering
Classes 8-10

3 Threat Hunting & Threat Modelling
Class 8

Core Activities
- Threat Hunting Methodology: Proactive TTP Identification in Simulated Environments
- MITRE ATT&CK Framework Application as Primary Intelligence Reference
- STRIDE & PASTA Threat Modelling Methodologies
- Attack Tree Construction & Cyber Kill Chain Analysis
- Threat Intelligence Brief Preparation

Labs & Tools
- MITRE ATT&CK Navigator (Free)
- STRIDE / PASTA Threat Modelling Templates
- Claude / ChatGPT — Threat Model Generation & Intelligence Briefs

3 OSINT — Open Source Intelligence Operations
Class 9

Core Activities
- Passive & Active OSINT Campaign Execution
- Target Profiling: Email Harvesting, DNS Reconnaissance, Subdomain Enumeration
- Social Media Footprinting
- OSINT Data Correlation & Target Profile Report Generation
- Legal & Ethical Constraints of Professional Intelligence Gathering

Labs & Tools
- Maltego Community Edition
- Spiderfoot (Open Source OSINT Automation)
- Claude / ChatGPT — Intelligence Gap Analysis

PHASE 3: Threat Intelligence, OSINT & Social Engineering

Classes 8-10

3 Social Engineering — Attack Techniques & Simulation

Class 10

Core Activities

- Social Engineering Attack Vectors: Phishing, Spear-Phishing, Vishing, Smishing, Pretexting, Baiting
- Real World Breach Case Study Analysis
- Phishing Site Construction Demonstration
- Defensive Awareness Strategies & Organizational Reporting Procedures

Labs & Tools

- Social Engineering Toolkit (SET)
- Zphisher
- Phishing Site Demo & Credential Harvesting Email Demo
- Claude / ChatGPT — Security Awareness Training Content Drafting

PHASE 4: Vulnerability Assessment & Penetration Testing

Classes 11-27

4 Network Security Assessment: Vulnerable Router & Honeypot

Class 11-13

Core Activities

- Structured Network Penetration Testing Against DVAR (tinysploitARM)
- Network Reconnaissance & Service Enumeration: Nmap SYN, UDP, Version Detection, NSE Script Scans
- Wireshark Traffic Analysis & Anomaly Identification
- Honeypot Architecture: Deployment, Testing & Deception Mechanism Analysis
- CVSS-Scored Vulnerability Documentation & Network Penetration Testing Report

Labs & Tools

- Damn Vulnerable ARM Router — DVAR / tinysploitARM (VulnHub)
- Nmap (Network Mapper)
- Wireshark (Traffic Analysis)
- Honeypot Sample Lab (Instructor-Provided)

4 Web Application Penetration Testing

Class 14-17

Core Activities

- OWASP Top 10 Systematic Mapping to Live Exploitation
- SQL Injection, XSS, Broken Authentication, Security Misconfiguration, SSRF
- Burp Suite: HTTP Interception, Repeater Manual Testing, Intruder Fuzzing
- PortSwigger Academy Labs — Supplementary Structured Practice
- Web Application Penetration Testing Report with Severity-Prioritised Findings

Labs & Tools

- OWASP Juice Shop
- WebGoat
- Burp Suite Community Edition
- PortSwigger Web Security Academy (Free)

PHASE 4: Vulnerability Assessment & Penetration Testing
Classes 11-27

4 Mobile Application Penetration Testing (APK)
Class 18-19

Core Activities
- Static Analysis: Hardcoded Credentials, Insecure Permissions, Exposed Application Components
- Dynamic Testing: Insecure Local Data Storage, Cleartext Network Transmission, Weak Authentication
- MobSF Automated Static Analysis Deployment
- OWASP Mobile Top 10 Finding Classification
- Professional Mobile Penetration Testing Report Production

Labs & Tools
- DIVA — Damn Insecure and Vulnerable Android App
- MobSF (Mobile Security Framework)
- Android Emulator / Physical Device

4 API Security Testing & Exploitation
Class 20-22

Core Activities
- OWASP API Security Top 10: BOLA/IDOR, Broken Authentication, Excessive Data Exposure, Broken Function Level Authorization, Injection
- API Reconnaissance & Request Crafting with Postman
- Burp Suite Intruder: Parameter Fuzzing & JWT Token Manipulation
- API Attack Surface Mapping & Endpoint Discovery
- Professional API Security Assessment Report (OWASP API Top 10 Classification)

Labs & Tools
- OWASP Juice Shop (API Endpoints)
- Postman (API Reconnaissance & Request Crafting)
- Burp Suite Community Edition (Intruder, Repeater)

PHASE 4: Vulnerability Assessment & Penetration Testing
Classes 11-27

4 System & Server Penetration Testing
Class 23-24

Core Activities
- MSMQ (Microsoft Message Queuing) Exploitation on Windows Server 2022
- Service Exploitation on Ubuntu Server
- Metasploit Framework: Structured Exploitation & Meterpreter Sessions
- Exploitation Evidence Collection & Professional System Penetration Testing Report

Labs & Tools
- Metasploit Framework
- Windows Server 2022 (Evaluation Licence)
- Ubuntu Server 22.04
- Metasploitable 2 & 3

4 Malware Analysis: Static & Dynamic Techniques
Class 25-26

Core Activities
- Malware Static Analysis: File Hashing, String Extraction, PE Header Review
- Dynamic Malware Analysis: Process Behavior, Registry Changes, Network Activity
- Sandbox Environment Execution
- IOC Identification & Threat Classification
- MITRE ATT&CK Mapping
- Malware Analysis Report Writing

Labs & Tools
- FatRat (Payload Generator)
- Veil Framework (AV Evasion)
- Static Analysis: PE header tools, String Extractor
- Dynamic Analysis: Process Monitor, Registry Monitor
- Any.run Sandbox (Free Tier)

PHASE 4: Vulnerability Assessment & Penetration Testing

Classes 11-27

4 Vulnerability Assessment — CVE Research, Scanning & Prioritization

Class 27

Core Activities

- CVE & CVSS Scoring Framework Analysis
- Structured Vulnerability Scanning Against Lab Infrastructure
- Scan Result Interpretation, Severity Prioritization & False Positive Validation
- NVD Cross-Referencing for Manual Verification
- Exploit Availability, Patch Status & Asset Criticality Assessment

Labs & Tools

- Nessus Essentials (Free)
- OpenVAS Community Edition
- NVD — nvd.nist.gov (CVE Reference Database)

PHASE 5: System Hardening & Security Assessment
Classes 28-31

5 Windows Defender Bypass & AV Evasion
Class 28

Core Activities
- Windows Defender Architecture & Detection Basics
- AV Evasion & Payload Obfuscation Concepts
- Defender Bypass Demonstration (Controlled Lab)
- MITRE ATT&CK Defense Evasion Mapping
- Ethical & Legal Considerations of AV Research

Labs & Tools
- Windows 11 / Windows Server 2022 (Defender Lab Environment)

5 Windows Server 2022: Active Directory Hardening
Class 29

Core Activities
- MSMQ Exploitation Overview on Windows Server 2022
- Active Directory Hardening with CIS Benchmarks
- Kerberoasting Mitigation & LDAP Security Configuration
- GPO & Audit Policy Optimization
- AD Security Assessment & Remediation Reporting

Labs & Tools
- Windows Server 2022 with Active Directory
- CIS Benchmark — Windows Server 2022 AD Controls
- Group Policy Management Console (GPMC)

PHASE 5: System Hardening & Security Assessment
Classes 28-31

5 Windows 11 Endpoint Hardening
Class 30

Core Activities
- CIS Benchmark Level 1 & Level 2 Controls for Windows 11 Endpoint
- Account Policies, Windows Firewall Advanced Configuration & BitLocker Encryption
- AppLocker Application Control & Security Baseline via Group Policy
- Pre- and Post-Hardening Vulnerability Scan Validation
- Structured CIS Compliance Report Production

Labs & Tools
- Windows 11 (CIS Benchmark Lab Environment)
- CIS Benchmark — Windows 11 Controls
- Group Policy Management Console (GPMC)

5 Ubuntu Server Hardening
Class 31

Core Activities
- Ubuntu Server CIS Benchmark Hardening (22.04)
- SSH, Filesystem & Package Security Configuration
- Kernel Tuning, User Policy & audit Logging Setup
- AppArmor MAC Profile Configuration & Testing
- OpenVAS Pre/Post Hardening Comparison & Security Reporting

Labs & Tools
- Ubuntu Server 22.04
- CIS Benchmark — Ubuntu Server Controls
- OpenVAS / Greenbone Community Edition (Pre/Post Hardening Scan)
- AppArmor (Mandatory Access Control)

PHASE 6: Artificial Intelligence & LLM Security Testing
Classes 32-33

6 LLM Security Testing & AI Red Teaming
Class 32-33

Core Activities

- OWASP Top 10 for LLMs 2025: Prompt Injection (Direct & Indirect), Jailbreaking, System Prompt Extraction
- Insecure Output Handling, Sensitive Data Leakage Testing
- Structured AI Red Teaming Methodology with Documented Findings
- Garak Automated LLM Vulnerability Assessment Deployment
- Professional LLM Security Assessment Report & Responsible Disclosure Documentation

Labs & Tools

- AImaginationLab / vulnerable-llms (GitHub)
- lonerzee / redteam-llm-lab (GitHub)
- Garak — Open Source LLM Vulnerability Scanner
- PortSwigger LLM Attack Labs
- llm-sec.dev (Supplementary Practice)

PHASE 7: Container & Cloud Infrastructure Security

Classes 34-35

7 Docker Container Penetration Testing

Class 34

Core Activities

- Docker Architecture & Container Security Analysis
- Privileged Container Misconfiguration & Weak Image Risks
- Docker Daemon Exposure & Security Misconfigurations
- Container Escape Techniques (Controlled Lab Only)
- DeepCE Container Privilege Escalation Practice
- Docker Security Assessment & CIS Benchmark Reporting

Labs & Tools

- Vulhub — Pre-Configured Vulnerable Docker Compose Stacks (vulhub.org)
- Deepce (Docker Container Privilege Escalation Tool)
- Docker Engine & Docker Compose
- CIS Docker Benchmark (Reference)

7 Introduction to Cloud Computing & Security

Class 35

Core Activities

- Cloud Computing Fundamentals: IaaS, PaaS, SaaS Service Models
- Deployment Models: Public, Private, Hybrid
- Shared Responsibility Model Across AWS, Azure & GCP
- Common Cloud Vulnerabilities: IAM Misconfigurations, Exposed S3/Blob Buckets, Privilege Escalation, Metadata Service Abuse
- Real-World Cloud Breach Case Study Analysis & Cloud Security Risk Summary Report Analysis

Labs & Tools

- Cloud Breach Case Study Analysis (Instructor Provided)
- AWS / Azure / GCP Free Tier (Conceptual Reference)
- Claude / ChatGPT

PHASE 8: Prompt Engineering & AI-Powered Security Tooling

Classes 36-37

8 Prompt Engineering & AI Security Tools

Class 36-37

Core Activities

- Advanced Prompt Engineering Techniques (Chain-of-Thought, Role Based, Few-Shot, Output Structuring)
- AI-Powered Security Tool Development
- Prompt Chaining for Multi-Step Security Workflows
- AI Security Tools Portfolio Documentation

Labs & Tools

- Claude • ChatGPT (OpenAI Free Tier)
- Real Security Datasets for Tool Validation

PHASE 9: Governance, Compliance & Security Frameworks

Class 38

9 Fundamentals of IT Governance & Compliance

Class 38

Core Activities

- IT Governance Frameworks: COBIT 2019, NIST CSF 2.0, ISO 27001 — Operational Application
- GDPR (Europe) & CCPA (USA) Data Protection Obligations
- Security Policy Development & Compliance Programme Design
- Audit Preparation Fundamentals
- Real-World Governance Case Study Exercise & Executive Governance Summary Report

Labs & Tools

- Governance Case Study (Instructor-Provided)
- NIST CSF 2.0 Framework Reference Document
- ISO 27001 Control Reference
- Claude / ChatGPT — Compliance Gap Analysis & Control Mapping

PHASE 10: Career Engineering & Offensive Security Readiness

Classes 39-40

10 Career Profile: LinkedIn, GitHub Portfolio & Resume

Class 39

Core Activities

- LinkedIn Profile: ATS-Aligned Keyword Strategy, Optimised Headline & Skills Endorsement Configuration
- GitHub Portfolio: Penetration Testing Write-Ups, Tool Scripts & AI Security Project Documentation
- Professional Offensive Security CV Drafting & ATS Scoring
- TryHackMe & HackTheBox Public Profile Evaluation as Employer-Facing Credentialing Assets
- Personal Brand Strategy for the Global Cybersecurity Job Market

Labs & Tools

- LinkedIn
- GitHub (Free Portfolio Repository)
- TryHackMe Public Profile
- HackTheBox Public Profile
- Jobscan / Teal / Resume Worded — ATS Optimisation Tools
- Claude / ChatGPT — Resume Tailoring & LinkedIn Content Generation

10 Job Hunting Strategies & Interview Mastery

Class 40

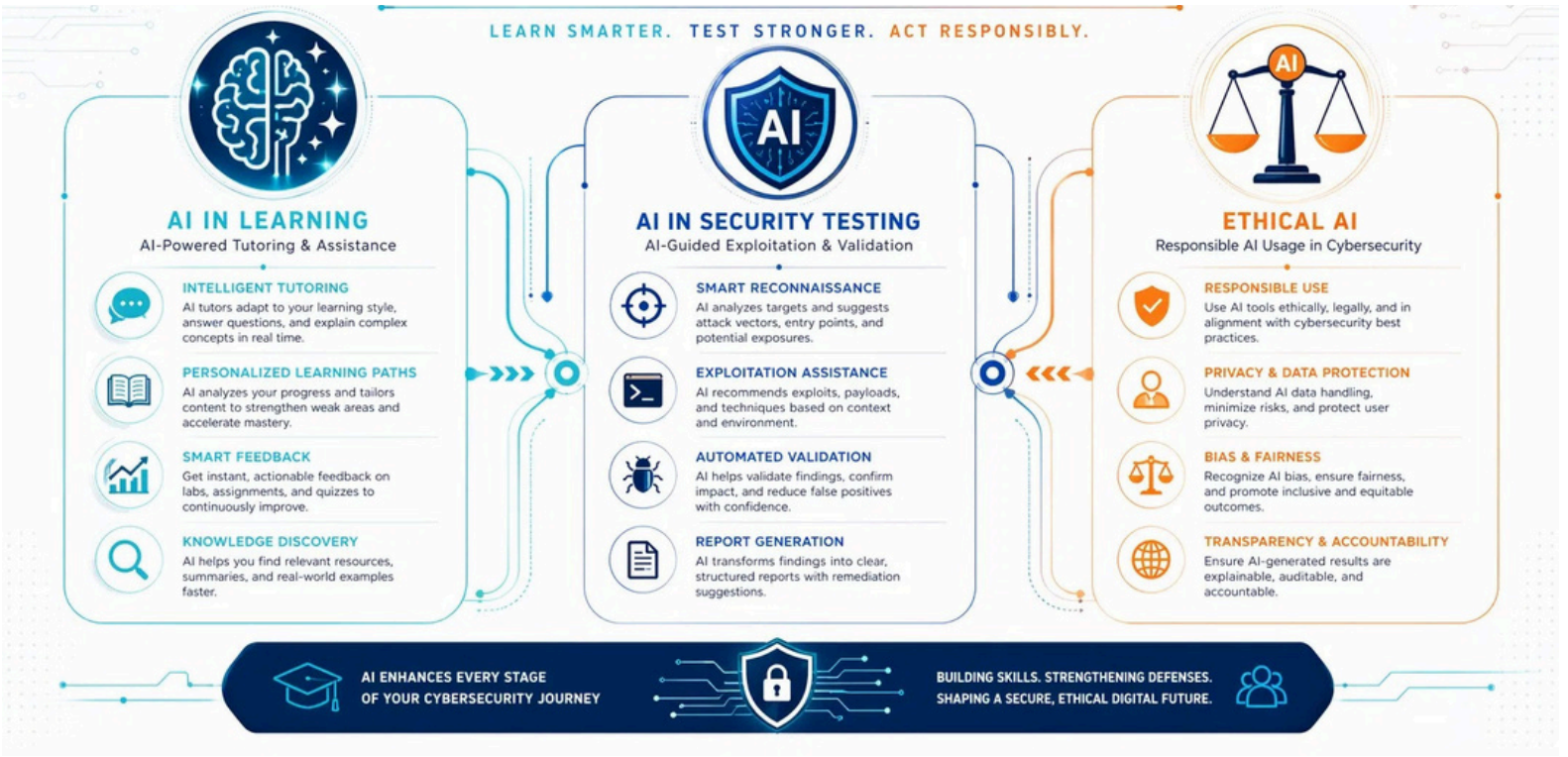
Core Activities

- Structured High-Volume Job Application Strategy: LinkedIn Easy Apply, Dice, CyberSecJobs, USAJobs, Indeed
- Cold Outreach Templates for Hiring Managers & Technical Recruiters
- Mock Technical Interviews: Penetration Tester & AI Red Team Operator Questions
- USA Cybersecurity Salary Negotiation Strategy with Benchmark Data
- Personalized 30-60-90 Day Job Search Plan & Success Roadmap

Labs & Tools

- LinkedIn, Dice, CyberSecJobs, USAJobs, Indeed (Job Platforms)
- Glassdoor — Salary Benchmarking
- CyberSeek Career Pathway
- Claude / ChatGPT — Mock Interview Practice & Salary Negotiation Script Generation

AI Integration Throughout



AI enhances every stage of your cybersecurity journey—from intelligent tutoring and smart reconnaissance to ethical red teaming and responsible disclosure practices.

Hands-On Labs & Capstone Project

Lab Environments

TryHackMe Rooms
Guided security challenges

All Levels

DVWA & PortSwigger
Web application vulnerabilities

Intermediate

Metasploitable
Penetration testing practice

Advanced

MobSF Labs
Mobileappsecurity testing

Intermediate

LLM Security Labs
AI/LLM vulnerability testing

Advanced

OverTheWire Bandit
Linux terminal skills

Beginner

Capstone Project

Full Penetration Testing Engagement

Execute acomplete end-to-end penetration test on a designated target, progressing systematically from reconnaissance through exploitation to privilege escalation.

Deliverables:

- Executive Summary for stakeholders
- Technical Findings with evidence
- CVSS Scoring & risk prioritization
- Remediation Recommendations
- Professional pentest report

AI-Generated Reporting

Leverage Alassistance to structure findings, prioritize by severity, and generate executive summaries for non-technical stakeholders.

95%
Job Placement

40%
Avg Salary Increase

9
Career Roles

Why Choose Transfotech Academy?

100% Hands-On
Reallabs,realtools,real-world scenarios

AI-Enhanced Learning
Personalized tutoring and smart assistance

Industry-Aligned
Curriculumreflectscurrentthreat landscape

Career-Ready
95%jobplacementratewithin 6 months

Expert Instructors
Certifiedprofessionalswithfield experience

Flexible Scheduling
18-week intensive or part-time options

Ready to Secure Your Future?

Join the next cohort of elite cybersecurity professionals trained by industry experts.

Enroll Now | Request Info