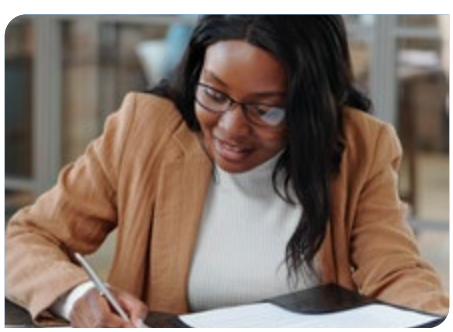
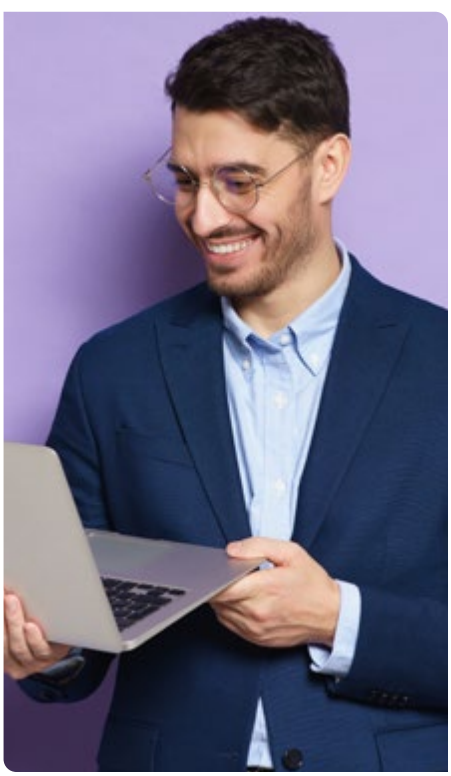
ThriveDX

Cyber Infrastructure & Penetration Testing Course





Cyber Infrastructure & Penetration Testing Course

Learning Method
Live (Online), Instructor-Led

Difficulty
Essentials

Duration
48 Hours

Pricing
$5,940

In the rapidly evolving domain of cybersecurity, the ability to proactively identify and exploit vulnerabilities is paramount. This offensive security course, meticulously designed around the practical art of penetration testing, equips participants with the cutting-edge techniques and tools required to breach defenses and enhance system security.

Spanning seven detailed modules, this course offers a thorough exploration from the foundational concepts of penetration testing to advanced strategies for securing Active Directory and cloud environments. Begin with essential penetration testing terminology and frameworks, advance through complex reconnaissance techniques using AI-powered tools, and learn to navigate and control network defenses with precision. The course culminates in effective strategies for reporting, remediation, and ensuring sustainable security improvements. Through practical exercises and real-world scenarios, learners are prepared to tackle complex security vulnerabilities, making them valuable assets in securing digital environments.

Who Should Attend:

- IT professionals
- Network and system administrators
- Aspiring cybersecurity experts and penetration testers
- Security analysts and consultants

Prerequisites:

- A basic understanding of computer networks and systems.
- Familiarity with Windows and Linux operating systems.
- An understanding of basic security concepts and practices.

Relevant for the Following Work Paths:

- Penetration and Vulnerability Tester
- Security Consultant
- Cybersecurity Analyst

Upon Completion, Participants Will Emerge With:

1

Master Penetration Testing Fundamentals: Understand penetration testing methodologies, legal and ethical considerations, and security frameworks.

2

Advanced Reconnaissance Skills: Master both active and passive reconnaissance techniques using AI-powered and open-source tools to gather critical information and assess vulnerabilities.

3

Effective Exploitation Techniques: Learn to exploit vulnerabilities through various attacks like password spraying, brute force, and custom exploit deployment to gain unauthorized access.

4

Enhanced Situational Awareness and Privilege Escalation: Develop skills in advanced environment enumeration and privilege escalation tactics for both Windows and Linux systems.

5

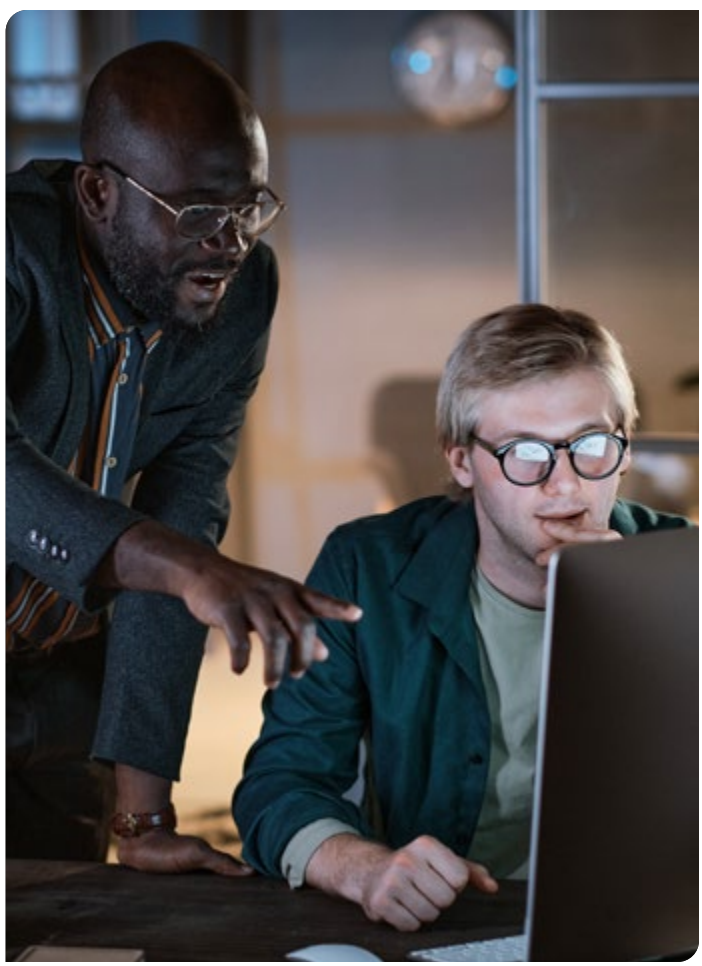
Advanced Access and Lateral Movement: Implement techniques for maintaining access, controlling compromised systems, and executing lateral movements within a network.

6

Domain and Cloud Infrastructure Dominance: Gain expertise in exploiting and dominating Active Directory and Azure environments, including cross-platform exploitation and security assessments.

7

Professional Reporting and Remediation: Enhance abilities in documenting penetration tests, analyzing risks, and formulating industry-standard remediation strategies.



Program Structure

Module 1

Penetration Testing Fundamentals

- Penetration Testing Terminology
- Legal and Ethical Frameworks
- Security Frameworks and Methodologies
- Types of Penetration Tests
- Cyber Attack Cycle and Attack Surfaces
- Industry Standards
- Penetration Testing Attacker Machine Essentials

Module 2

Reconnaissance and Information Gathering

- Active and Passive Reconnaissance Techniques
- Open Source Scanning Tools
- Network Topology Discovery
- OS and Service Fingerprinting
- Vulnerability Scanning and Analysis
- Situational Awareness and Monitoring
- Utilizing AI-Powered Reconnaissance Tools

Module 3

Gaining a Foothold

- Bypassing Network Security Measures
- Exploiting Vulnerable Services
- Public and Custom Exploit Deployment
- Password Spray, Brute Force Attacks, and Credential Stuffing
- Adversary in the Middle (AITM) Attacks
- Password Cracking, Known Wordlists, Rainbow Tables, and Third Party Services

Module 4

Situational Awareness and Privilege Escalation

- Advanced Environment Enumeration
- Security Infrastructure Discovery
- Tactical Tool Infiltration
- Windows and Linux Privilege Escalation Techniques
- On-Prem and Hybrid Active Directory Enumeration

Module 5

Persistency and Lateral Movement

- Advanced Techniques for Establishing and Maintaining Access
- Command and Control (C2) Setup
- Tunneling and Pivoting Techniques
- Credential Access and Reuse Techniques
- Lateral Movement via Pass-the-Hash and Pass-the-Ticket
- Session Hijacking for Lateral Movement
- Exploiting Trust Relationships
- Remote Execution Tools and Techniques

Module 6

Domain Active Directory and Azure Takeover

- Active Directory Exploitation Techniques
- Azure Active Directory and Cloud Infrastructure Exploitation
- Cross-Platform Exploitation and Access
- Advanced Domain Persistence and Dominance Techniques
- Manipulating Azure AD Connect
- Exploitation of Trusts and Federated Services
- Comprehensive Audit and Security Posture Assessment

Module 7

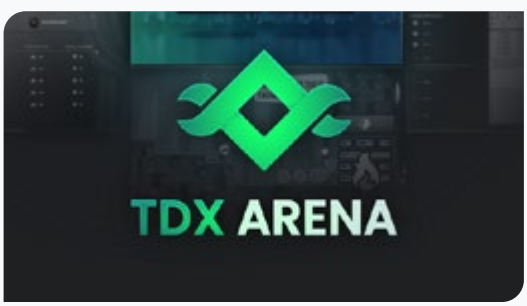
Reporting, Remediation, and Follow-Up

- Documenting Penetration Tests
- Risk Analysis and Prioritization
- Developing Remediation Strategies
- Industry-Backed Remediation Recommendations

Certification Readiness

All participants completing the course will receive a **ThriveDX Course Completion Certification**. Participants completing the final accreditation exam will also receive a **ThriveDX Penetration Tester Certification**. This course also provides practical knowledge for completing the GIA Penetration Tester (GPEN) certification.

Note: The certification subjects may change based on the certification provider, and additional study and research may be necessary to meet certification requirements.



Embedded Labs and Challenges

The course includes our state-of-the-art proprietary cloud-based digital education platform, **TDX Arena**, in which real-life scenarios and advanced tech teaching meet in a gamified environment.

TDX