APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

HTB Certified Active Directory Pentesting Expert (CAPE) Training

Hack The Box Authorized Training · Applied Technology Academy

Our successful training results keep our corporate and military clients returning. That's because we provide everything you need to succeed. This is true for all of our courses.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Advanced	**eLearning**	**1 year: Penetration Tester**	**$120,000**	**Yes**

Course Overview

The HTB Certified Active Directory Pentesting Expert (HTB CAPE) is a highly hands-on certification assessing candidates' skills in identifying and exploiting advanced Active Directory (AD) vulnerabilities. HTB CAPE certification holders will possess technical competency in AD and Windows penetration testing, understanding complex attack paths, and employing advanced techniques to exploit them. HTB CAPE certification holders will demonstrate proficiency in executing sophisticated attacks abusing different authentication protocols such as Kerberos and NTLM and abusing misconfigurations within AD components and standard applications in AD environments such as Active Directory Certificate Services (ADCS), Windows Update Server Services (WSUS), Exchange, and Domain Trusts. Furthermore, they will be adept at leveraging specialized tools to exploit AD from Linux and Windows and utilizing Command and Control (C2) frameworks for post-exploitation operations. They will also be able to conduct internal penetration tests professionally against modern AD environments.

The HTB CAPE certification represents the next step in advancing in AD pentesting beyond the HTB Certified Penetration Testing Specialist (HTB CPTS) certification.

Course Outline

The certification is earned through the Active Directory Penetration Tester job-role path — 15 modules, each with its own hands-on skills assessment.

- 1. Active Directory Enumeration & Attacks (Medium)
- 2. Active Directory LDAP (Medium)
- 3. Active Directory PowerView (Medium)
- 4. Active Directory BloodHound (Medium)
- 5. Windows Lateral Movement (Medium)
- 6. Using CrackMapExec (Medium)
- 7. Kerberos Attacks (Hard)
- 8. DACL Attacks I (Hard)

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- 9. DACL Attacks II (Hard)
- 10. NTLM Relay Attacks (Hard)
- 11. ADCS Attacks (Hard)
- 12. Active Directory Trust Attacks (Hard)
- 13. Intro to C2 Operations with Sliver (Hard)
- 14. Introduction to Windows Evasion Techniques (Hard)
- 15. MSSQL, Exchange, and SCCM Attacks (Hard)

Intended Audience

- Senior Penetration Testers
- Windows & Active Directory Penetration Testers
- Red Team Operators
- Active Directory Security Specialists
- System Administrators
- Cybersecurity Consultants
- Security Analysts

Prerequisites

The following is a list of prerequisites for a successful outcome:

- Interpreting a letter of engagement
- Advanced knowledge of Active Directory infrastructure and security concepts
- Knowledge around Windows and Active Directory and their functionality
- Understanding Active Directory authentication protocols (Kerberos, NTLM, LDAP, Certificate based-authentication, etc.)
- Familiarity with common and advanced Active Directory attacks and exploitation techniques
- Proficiency in navigating complex AD structures and understanding AD permissions and policies
- Ability to detect and exploit misconfigurations in Active Directory environments
- Knowledge of bypass techniques to circumvent various security measures in Windows environments
- Capability to recommend and implement security hardening measures for AD
- Professionally communicating and reporting vulnerabilities

Follow-On Courses

Hack The Box Certified Web Exploitation Expert (HTB CWEE)

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Knowledge Domains

- Advanced Active Directory Enumeration
- Advanced Active Directory Attacks
- Abusing AD Protocols
- Abusing AD Trusts
- Abusing AD Misconfigurations
- Abusing Common Active Directory Components
- Command and Control (C2) Operations
- Windows Evasion
- Pivoting & Lateral Movement
- Advanced Post-exploitation Tactics

The Exam

Candidates perform an internal penetration test against a real-world enterprise Active Directory network hosted in HTB's infrastructure and reached over VPN, using Pwnbox or their own VM. A letter of engagement states the objectives and scope.

Eligibility requires 100% completion of the Active Directory Penetration Tester job-role path first — evaluation happens throughout the path, not only at the exam.

Exploitation alone does not pass: candidates must submit a commercial-grade report explaining how each vulnerability was identified and exploited, and propose remediation.

The whole process runs in the browser through Pwnbox, with no infrastructure or tooling requirements of your own.

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.