Certified Active Directory Pentesting Expert

Course Duration: e-learning
Exam Reference: HTB-CAPE

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.

Prerequisites

- 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

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Certified Active Directory Pentesting Expert

Course Objectives

- Conduct Advanced Active Directory Assessments: Learn to audit Active Directory security, identify inefficiencies in its configurations and Group Policies, and enumerate complex networks.
- Execute Privilege Escalation and Lateral Movement: Master techniques for gaining higher privileges and moving laterally across networks after initial access.
- Assess and Exploit Common Services: Assess the security of services like Active Directory Certificate Services (ADCS), Exchange, and MSSQL to find and exploit vulnerabilities.
- Evade Defenses and Chain Vulnerabilities: Develop skills to bypass Windows security measures and chain multiple network vulnerabilities to achieve your objectives.
- Perform Professional Post-Exploitation and Reporting: Utilize Command and Control (C2) frameworks for post-exploitation activities and learn to professionally report all identified vulnerabilities.

Course Outline

Module 1: Active Directory Enumeration & Attacks

- Active Directory LDAP
- Active Directory PowerView
- Active Directory BloodHound

Module 2: Windows Lateral Movement

- Using CrackMapExec

Module 3: Kerberos Attacks

- DACL Attacks I
- DACL Attacks II
- NTLM Relay Attacks
- ADCS Attacks
- Active Directory Trust Attacks

Module 4: Post-Exploitation and Evasion

- Intro to C2 Operations with Sliver
- Introduction to Windows Evasion Techniques
- MSSQL, Exchange, and SCCM Attacks