Certified Ethical Hacker Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

{*training} is the world's first AI-integrated ethical hacking certification, designed to boost cybersecurity productivity by 40% and double operational efficiency. Through its 5 AI-augmented phases—reconnaissance, scanning, gaining access, maintaining access, and covering tracks—you'll master both core and advanced hacking strategies.

Gain practical experience via 220+ labs, 550+ attack techniques, and 4,000+ tools. Validate your expertise through global Capture the Flag (CTF) competitions and complete your journey with a **6-hour hands-on exam** or **4-hour knowledge exam**.

Recognized by **DoD 8140**, **ANAB 17024**, and **NCSC**, this certification aligns with **NICE 2.0** and **NIST** frameworks.

Prerequisites

- Minimum 2 years of IT security experience
- Strong TCP/IP fundamentals
- CompTIA Security+ or CND training recommended

Who Should Attend

- Cybersecurity professionals advancing their AI-powered security skills
- Teams aiming to outpace threat actors with AI automation
- Government and military units seeking accredited certifications
- Security officers, auditors, admins, pen testers, and IT defenders

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Ethical hacking methodologies enhanced with AI automation
- Hands-on skills to apply AI across all five hacking stages
- Tools for predictive threat analysis and automated anomaly detection
- Real-world CTF challenges to validate your readiness

Certified Ethical Hacker Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Outline

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service Attacks
- Session Hijacking
- IDS, Firewalls & Honeypots Evasion
- Hacking Web Servers
- Web Application Exploits
- SQL Injection
- Hacking Wireless Networks
- Mobile Platform Hacking
- IoT Attacks
- Cloud Security
- Cryptography