Advanced Ethical Hacking and Penetration Testing Training Course



19 - 23 Oct 2026

Boston

7500 € (Per Person)

Ref: #CYB5585_87790

Course Introduction / Overview:

This intensive training course provides a comprehensive exploration of the principles and practices of ethical hacking and penetration testing. In an era of escalating cyber threats, organizations require skilled professionals who can think like an attacker to identify and mitigate vulnerabilities before they are exploited. This program is designed to move beyond theoretical knowledge, immersing participants in hands-on labs and real-world simulations that mirror complex enterprise environments. Drawing upon established methodologies like the Penetration Testing Execution Standard (PTES), the curriculum covers everything from initial reconnaissance and network scanning to advanced exploitation and post-exploitation techniques. As detailed in seminal works like "The Web Application Hacker's Handbook" by Dafydd Stuttard, a proactive security posture is non-negotiable. BIG BEN Training Center has structured this course to equip attendees with the practical skills and ethical framework necessary to conduct thorough security assessments, providing actionable intelligence to strengthen organizational defenses and ensure robust digital resilience against sophisticated adversaries.

Target Audience / This training course is suitable for:

- Information Security Analysts and Managers.
- Penetration Testers and Ethical Hackers.
- Network Administrators and Engineers.
- Security Auditors and Consultants.
- IT Professionals seeking to specialize in cybersecurity.
- Software Developers and Application Security Specialists.
- System Administrators responsible for security.
- Cybersecurity enthusiasts and career changers.

Target Sectors and Industries:

- Financial Services and Banking.
- Information Technology and Telecommunications.
- Healthcare and Pharmaceutical.
- Government Agencies and Public Sector Bodies.
- Energy, Oil, and Gas.
- Retail and E-commerce.
- Consulting and Professional Services.
- Defense and Aerospace.

Target Organizations Departments:

- Information Technology (IT) and Infrastructure.
- Information Security and Cybersecurity.
- Internal Audit and Compliance.
- Risk Management.
- Software Development and Engineering.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Research and Development.

Course Offerings:

By the end of this course, the participants will have able to:

- Master the phases of a professional penetration test, from scoping to reporting.
- Utilize advanced network scanning and enumeration techniques to map target environments.
- Identify and exploit common vulnerabilities in web applications, such as SQL injection and XSS.
- Conduct sophisticated system hacking and privilege escalation attacks.
- Analyze and bypass network security controls like firewalls and intrusion detection systems.
- Perform security assessments on wireless networks and mobile platforms.
- Develop custom scripts to automate security testing tasks.
- Compile comprehensive and actionable penetration testing reports for technical and executive audiences.
- Apply a strict ethical framework to all security assessment activities.

Course Methodology:

The training methodology at BIG BEN Training Center is centered on immersive, hands-on learning to ensure participants develop practical, real-world skills. This course heavily emphasizes a lab-based environment where attendees will spend a significant portion of their time applying concepts and techniques against a variety of simulated targets. The approach is highly interactive, featuring a blend of expert-led instruction, live demonstrations of hacking tools and techniques, and individual and group-based exercises. We utilize complex case studies drawn from actual security incidents to provide context and challenge participants' problem-solving abilities. Collaborative teamwork is encouraged through red team versus blue team scenarios, fostering communication and strategic thinking. Throughout the course, instructors provide continuous feedback and personalized guidance, ensuring that every participant can overcome challenges and master the learning objectives. This dynamic and engaging methodology transforms theoretical knowledge into tangible, job-ready expertise in the field of ethical hacking.

Course Agenda (Course Units):

Unit One: Foundations of Ethical Hacking and Reconnaissance

- Introduction to Ethical Hacking and Legal Frameworks.
- Understanding the Cyber Kill Chain and Attack Vectors.
- Mastering the Penetration Testing Execution Standard (PTES).
- Passive Reconnaissance and Open-Source Intelligence (OSINT) Gathering.
- Active Reconnaissance Techniques and Footprinting.
- Advanced Network Scanning with Nmap and other tools.
- Vulnerability Identification and Analysis.

Unit Two: Gaining Access and System Exploitation

- System Hacking Methodologies and Password Cracking Techniques.
- Gaining Access using Metasploit and Exploit Frameworks.
- Understanding Malware, Trojans, and Backdoors.
- Social Engineering Tactics and Countermeasures.
- Introduction to Web Application Architecture and Technologies.
- Exploiting Common Web Vulnerabilities like SQL Injection (SQLi).
- Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) Attacks.

Unit Three: Advanced Network and Web Application Attacks

- Evading Intrusion Detection Systems (IDS), Firewalls, and Honeypots.
- Advanced Session Hijacking and Man-in-the-Middle Attacks.
- Hacking Wireless Networks (WEP, WPA, WPA2/3).
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks.
- Advanced Web Application Exploitation Techniques.
- Attacking Authentication and Authorization Mechanisms.
- File Inclusion and Command Injection Vulnerabilities.

Unit Four: Post-Exploitation, Cloud, and Mobile Security

- Maintaining Access with Backdoors and Rootkits.
- Privilege Escalation on Windows and Linux Systems.
- Pivoting and Lateral Movement within a Compromised Network.
- Covering Tracks and Clearing Logs.
- Introduction to Cloud Penetration Testing (AWS, Azure).
- Fundamentals of Mobile Application Penetration Testing (iOS/Android).
- Identifying and Exploiting Insecure API Endpoints.

Unit Five: Reporting, Automation, and Modern Threats

- Crafting Professional Penetration Testing Reports.
- Remediation and Post-Assessment Activities.
- Introduction to Exploit Development Concepts.
- Automating Security Tasks with Python and Bash Scripting.
- Analyzing Advanced Persistent Threats (APTs).
- Introduction to IoT and Operational Technology (OT) Security.
- Comprehensive Capture The Flag (CTF) Capstone Challenge.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As offensive security tools become more automated and accessible, how does the role of the ethical hacker evolve to provide value beyond what a machine can discover?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by focusing on the strategic mindset of an attacker rather than merely teaching the mechanics of security tools. While participants will gain proficiency with industry-standard software, the core emphasis is on critical thinking, problem-solving, and adapting to dynamic environments. Unlike courses that present a rigid, checklist-based approach, our curriculum is built around a fluid, intelligence-driven methodology that mirrors the tactics of real-world adversaries. We delve deeply into the "why" behind an exploit, not just the "how," ensuring a profound understanding of vulnerability root causes. The program integrates a strong ethical component throughout, preparing participants not just to be skilled testers but also trusted security advisors. Furthermore, the course culminates in a comprehensive capstone challenge that requires attendees to synthesize all learned skills in a realistic, multi-stage penetration test, providing an unparalleled experience that solidifies knowledge and builds true confidence in their abilities.