# Ethical Hacking & Penetration Testing Professional Training Course

**Ref: #CYB3978**

## Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals with the hands-on knowledge and practical skills required to perform professional penetration testing and ethical hacking. In an increasingly complex threat landscape, a proactive security posture is essential. This program goes beyond theoretical concepts and focuses on the methodologies and tools used by real-world ethical hackers. Participants will learn how to simulate a full-scale cyberattack, from reconnaissance and vulnerability scanning to exploitation and post-exploitation. We will cover key topics like network penetration, web application security, and reporting to senior management. Drawing from the academic work of renowned authors like Peter Kim and his book "The Hacker Playbook," this program provides a strategic and practical framework for finding and fixing vulnerabilities before malicious actors can exploit them. His work emphasizes the importance of a structured approach to ethical hacking, just as a professional athlete follows a playbook. This course at BIG BEN Training Center will empower you to identify and mitigate security flaws and strengthen your organization's defenses.

## Target Audience / This training course is suitable for:

- Penetration testers.
- Ethical hackers.
- Cybersecurity analysts.
- Security engineers.
- IT auditors.
- Network administrators.
- Security consultants.

## Target Sectors and Industries:

- Technology and software.
- Financial services.
- E-commerce.
- Telecommunications.
- Managed security service providers.
- Government agencies and equivalents.
- Defense and military.

## Target Organizations Departments:

- Information Security.
- Security Operations Center (SOC).
- IT Audit.
- Product Security.
- Risk Management.
- Red Team.
- Application Development.

## Course Offerings:

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

- Conduct a comprehensive penetration test.
- Perform reconnaissance and information gathering.
- Identify and exploit network and application vulnerabilities.
- Create a professional penetration testing report.
- Communicate security risks to stakeholders.
- Use industry-standard penetration testing tools.
- Apply ethical hacking methodologies to secure systems.

## Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, lab-intensive methodology that simulates real-world attack scenarios. The program includes a series of capture-the-flag exercises and challenges where participants will apply hacking techniques in a safe and controlled environment. You will learn to use a variety of open-source and commercial tools to perform everything from network mapping to privilege escalation. The course emphasizes a structured, repeatable methodology, teaching you to think like a hacker while maintaining an ethical and professional mindset. The instructor will provide expert guidance and feedback throughout the labs, ensuring that you develop the critical thinking and problem-solving skills required for high-stakes security roles. This approach ensures the knowledge and skills gained are directly applicable to securing corporate networks and applications.

## Course Agenda (Course Units):

### Unit One: The Ethical Hacking Methodology

- Introduction to ethical hacking.
- The penetration testing lifecycle.
- Reconnaissance and information gathering.
- Scanning and enumeration.
- Vulnerability analysis.
- Planning a penetration test.
- Case study: a full-scale penetration test.

## Unit Two: Network Penetration Testing

- Network scanning and mapping.
- Exploiting network services.
- Password attacks.
- Wireless network security.
- Denial of service (DoS) and DDoS attacks.
- Post-exploitation techniques.
- Practical lab: a network penetration exercise.

## Unit Three: Web Application Security

- The OWASP Top 10.
- Common web application vulnerabilities (e.g., SQL injection).
- Cross-site scripting (XSS).
- Secure API testing.
- Authentication and session management.
- Using web application proxies.
- Practical lab: a web application penetration test.

## Unit Four: Post-Exploitation and Lateral Movement

- Maintaining persistence.
- Pivoting and lateral movement.
- Privilege escalation.
- Data exfiltration.
- Covering your tracks.
- Reporting findings to management.
- Case study: a post-exploitation scenario.

### Unit Five: The Final Report and Future Trends

- The structure of a penetration test report.
- Communicating risks to stakeholders.
- Remediation and mitigation strategies.
- The future of ethical hacking.
- Emerging threats.
- Final project: a comprehensive report.
- Legal and ethical considerations.
- Frequently Asked Questions:

## 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:

While a penetration test provides a snapshot of an organization's security at a single point in time, how can CISO ensure that these findings lead to a sustained improvement in security posture rather than a temporary fix?

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

This course stands out by providing a unique and vital focus on the practical, hands-on skills of penetration testing. Unlike theoretical courses, this program is designed to turn participants into professional ethical hackers. The curriculum is built around a series of realistic lab environments and capture-the-flag exercises. It teaches you to use the same tools and methodologies as real-world attackers to find and fix vulnerabilities. The emphasis on a structured, repeatable methodology and professional reporting distinguishes this course from others. It is for professionals who are ready to move beyond a defensive mindset and proactively test their organization's security to ensure it can withstand the most sophisticated attacks.