Hacking 101: Check Point Certified PenTesting Associate (CCPA)

Course Duration : 24 Hours **Course code : CCPA-H101**

1. Course Overview

The **Hacking 101: Check Point Certified PenTesting Associate (CCPA)** course introduces learners to the fundamentals of ethical hacking and penetration testing. This course focuses on understanding attack techniques, identifying vulnerabilities, and performing basic penetration tests in a controlled and legal environment using industry-standard tools and methodologies.

2. What you'll learn?

- Application security fundamentals
- Common web application vulnerabilities
- Secure coding best practices
- OWASP Top 10 threats
- Integrating security into DevOps
- Application threat detection and prevention

3. Target Audience

- Ethical hacking fundamentals
- Penetration testing methodologies
- Common attack techniques
- Vulnerability identification
- Basic exploitation techniques
- Reporting and documentation

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

4. Pre-Requisites

- Basic understanding of networking
- Familiarity with operating systems
- Interest in cybersecurity and ethical hacking

5. Course Content (Modules)

Module 1: Introduction to Ethical Hacking

- Ethics and legal considerations
- Penetration testing overview

Module 2: Reconnaissance and Information Gathering

- Passive and active reconnaissance
- Foot printing techniques

Module 3: Scanning and Enumeration

- Network scanning
- Service and vulnerability enumeration

Module 4: Exploitation Basics

- Common exploit techniques
- Exploitation tools overview

Module 5: Post-Exploitation Fundamentals

- Maintaining access
- Privilege escalation basics

Module 6: Reporting and Best Practices

- Documentation and reporting
- Pen-testing best practices

Module 7: Basic Troubleshooting and Maintenance

- Common firewall issues
- System maintenance tasks

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com