Infrastructure Hacking Check Point Certified Pen Testing Expert (CCPE)

Course Duration : 32 Hours **Course code : CCPE-INFRA**

1. Course Overview

The **Infrastructure Hacking Check Point Certified PenTesting Expert (CCPE)** course provides advanced skills to perform professional penetration testing on enterprise infrastructure. This course focuses on exploiting complex network, server, and Active Directory vulnerabilities using real-world attack techniques while following ethical hacking standards and reporting best practices.

2. What you'll learn?

- Advanced infrastructure penetration testing techniques
- Network and service exploitation
- Active Directory attacks and abuse
- Privilege escalation and lateral movement
- Persistence techniques
- Professional reporting and mitigation strategies

3. Target Audience

- Penetration testers
- Red team professionals
- Ethical hackers
- Cybersecurity consultants
- Security engineers

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

4. Pre-Requisites

- Strong networking and security knowledge
- Experience with ethical hacking tools
- Understanding of Windows and Linux systems

5. Course Content (Modules)

Module 1: Advanced Network Exploitation

- Deep scanning and enumeration
- Exploiting network services

Module 2: Active Directory Attacks

- Credential harvesting
- Kerberos and domain attacks

Module 3: Server and Infrastructure Exploitation

- Service misconfigurations
- Exploit chaining

Module 4: Privilege Escalation Techniques

- Windows and Linux escalation
- Kernel and service abuse

Module 5: Lateral Movement and Persistence

- Moving across enterprise networks
- Maintaining access

Module 6: Detection Evasion and Reporting

- Anti-detection techniques
- Professional penetration test reporting