BH
Security
Plus

eJPT v2

eLearnSecurity JUNIOR PENETRATION TESTER v2

☎ +91 77040 85057 bhsecurityplus.com Uttar Prddesh , India

INTRODUCTION

Welcome to the eLearnSecurity Junior Penetration Tester (eJPT) training program, your entry point into the dynamic world of penetration testing. In today's digital age, where cybersecurity is paramount, there is a rising demand for adept professionals who can assess and fortify network security. The eJPT certification equips you with the knowledge and skills needed to understand the fundamentals of penetration testing, enabling you to identify vulnerabilities, conduct security assessments, and fortify networks against cyber threats.

WHY CHOOSE eJPT V2?

The eLearnSecurity Junior Penetration Tester (eJPT) certification stands as a pinnacle in the realm of penetration testing proficiency. By participating in this program, you will:

- Dive deep into the intricacies of penetration testing principles and methodologies, covering essential areas such as reconnaissance, scanning, enumeration, exploitation, and post-exploitation techniques.
- Benefit from the seasoned guidance of certified instructors renowned for their expertise in cybersecurity. Our instructors bring extensive practical experience to the table, ensuring comprehensive learning.
- Hone your practical skills through immersive hands-on exercises and real-world simulations. You'll have ample opportunities to apply your knowledge in simulated environments, refining your penetration testing techniques in a safe and controlled setting.

WHO SHOULD ATTEND?

The eLearnSecurity Junior Penetration Tester (eJPT) training program caters to:

- IT professionals seeking to enhance their penetration testing skills and advance in their careers.
- Network administrators responsible for securing and maintaining network infrastructures.
- Cybersecurity enthusiasts and professionals looking to formalize their skills with industry-recognized certification.
- Individuals interested in entering the field of cybersecurity and specializing in penetration testing to mitigate cyber threats effectively.

COURSE OVERVIEW

Our eJPT V2 training program consists of 4 modules, covering a wide range of topics, including:

- Assessment Methodologies
- Network and Host Auditing
- Network and Host Penetrating Testing
- Web Application Penetration Testing

Each module is designed to provide you with the knowledge and skills necessary to excel in the field of ethical hacking.

JOIN US TODAY

Are you ready to elevate your Linux system administration skills? Embark on this thrilling journey with us and become a Red Hat Certified System Administrator (RHCSA). Enroll now and open doors to limitless opportunities in the fast-evolving realm of IT infrastructure management.

MODULE 1: ASSESSMENT METHODOLOGIES

- ·Information gathering (Reconnaissance)
- ·Footprinting and Scanning
- ·Different Methods Used by Hacker in Footprinting
- ·Locate endpoints on a Network
- ·Discover Open Ports and Services Available on a Target.
- ·Determine the operating system used by target.
- ·Extract company information from public sources.
- ·Gather Email Addresses from Public Sources
- ·Gather Technical Information
- ·Advance Google Hacking/Dorking
- ·Enumeration
- ·Enumeration Techniques
- ·Retrieve User Account details from the Target System
- ·Vulnerability Assessment/Analysis
- Vulnerability Assessment Life Cycle

MODULE 2: NETWORK AND HOST AUDITING

- ·Auditing Concepts
- ·Types of Audits
- ·Tools and Techniques
- ·Compliance Audits
- ·Security Awareness
- ·Packet Sniffing
- ·Wireshark
- ·Tcpdump
- Tshark

MODULE 3: NETWORK AND HOST PENETRATING TESTING

- ·Host Based Attack
- ·Network Based Attack
- ·Password Brute Forcing
- ·Custom Wordlist Generator with Crunch
- ·Custom Wordlist Generator with Cewl
- ·Password Cracking with Hashcat
- ·Password Cracking with John the Ripper
- ·Metasploit Framework
- ·Identify Vulnerability and Exploitation
- ·Exploit Database
- ·File Sharing to and from Target System.
- ·Gather Hashed Password Data from the Target
- ·Privilege Escalation
- ·Post Exploitation
- Social Engineering

MODULE 4: WEB APPLICATION PENETRATION TESTING

- ·Web Concepts
- ·Introduction to HTTP Protocol
- ·Reconnaissance on Web Application
- ·Discover Hidden Files and Directories
- ·Discover Sub-domain using Ffuf
- ·Introduction to Burp Suite
- ·Burp Suite Setup and Working
- ·Brute Force attack on HTTP Login Post Form
- ·Web Application Vulnerability
- ·OWASP Top 10
- ·Directory Traversal
- ·Finding Hidden Content
- ·Local File Inclusion
- ·Remote File Inclusion
- ·Command Injection
- ·File Upload Vulnerability

MODULE 4: WEB APPLICATION PENETRATION TESTING

- ·Web Concepts
- ·Introduction to HTTP Protocol
- ·Reconnaissance on Web Application
- ·Discover Hidden Files and Directories
- ·Discover Sub-domain using Ffuf
- ·Introduction to Burp Suite
- ·Burp Suite Setup and Working
- ·Brute Force attack on HTTP Login Post Form
- ·Web Application Vulnerability
- ·OWASP Top 10
- ·Directory Traversal
- ·Finding Hidden Content
- ·Local File Inclusion
- ·Remote File Inclusion
- ·Command Injection
- ·File Upload Vulnerability

CONTACT US

Official Website

www.bhsecurityplus.com

Official Youtube Channel

BH Security Plus

Official Instagram

BH Security Plus

Official Linkedin

BH Security Plus

Official Telegram

BH Security Plus

Official Twitter

BH Security Plus

+91 77040 85057,+91 9236044409

Bhsecplus@gmail.com ,
info@bhsecurityplus.com