CYBERIUM

eLearn Security

Junior Penetration Tester

eJPTv2

INTRODUCTION

The eJPTv2 (eLearnSecurity Junior Penetration Tester version 2) course is a comprehensive, hands-on training program designed for individuals looking to break into the field of penetration testing and cybersecurity. Created by eLearnSecurity, the eJPTv2 is a well-rounded, entry-level certification that offers learners a solid foundation in ethical hacking techniques, real-world pentesting skills, and essential tools used by security professionals.

This course is ideal for individuals who are new to penetration testing or cybersecurity and want to build practical skills that are essential in the security field. Whether you're an aspiring ethical hacker, IT professional, or someone transitioning into cybersecurity, the eJPTv2 provides the knowledge and experience required to understand and perform penetration testing in a controlled and ethical manner.

Completing the eJPTv2 course not only helps you gain practical penetration testing skills but also provides a strong foundation for pursuing more advanced certifications, such as the OSCP (Offensive Security Certified Professional). The knowledge gained in this course will be invaluable as you continue to build your skills and advance in the cybersecurity field.

The course simulates real-world attack scenarios, allowing learners to engage with security challenges similar to those they would face on actual penetration testing assignments. From discovering vulnerabilities in networks to exploiting web application flaws, you'll learn to approach each step of the process methodically and effectively.

Overview of eJPTv2 exam

The eLearnSecurity Junior Penetration Tester (eJPT) v2 exam is a practical, hands-on test designed to evaluate the skills and knowledge of individuals in the field of penetration testing. The exam consists of 35 questions and covers four key domains:

1. **Assessment Methodologies**
2. **Host and Network Auditing**
3. **Host and Network Penetration Testing**
4. **Web Application Penetration Testing**

The exam duration is 48 hours, allowing candidates to tackle practical challenges that mirror real-world penetration testing scenarios. During this time, candidates must demonstrate their ability to assess vulnerabilities, exploit weaknesses, and conduct audits across various systems and network environments. The test is designed to validate a candidate's understanding of penetration testing methodologies, tools, and techniques.

This exam is ideal for individuals pursuing a career in penetration testing or cybersecurity and looking to showcase their abilities in a structured and comprehensive environment

Course duration- 80 Hours

eJPTv2 SYLLABUS

Module 01- Introduction to Penetration Testing

1. **Overview of Penetration Testing**
2. **Rules of Engagement (ROE)**
3. **Understanding the Testing Lifecycle**
4. **Setting Up the Lab Environment**

Module 02- Information Gathering

1. **Passive and Active Reconnaissance**
2. **Identifying Open Ports and Services**
3. **Footprinting and Scanning**
4. **Gathering Information from Public Sources**
5. **Enumerating Network and Domain Data**

Module 03- Enumeration

1. **Banner Grabbing and OS Fingerprinting**
2. **Enumerating Users and Shared Resources**
3. **Network Mapping and Protocol Identification**
4. **System-Specific Information Collection**

Module 04- Vulnerability Assessment

1. **Identifying Vulnerabilities in Network Services**
2. **Utilizing Scanning Tools (e.g., Nessus, OpenVAS)**
3. **Manual Vulnerability Verification**
4. **Evaluating Risk and Impact of Vulnerabilities**

Module 05- Host-Based Exploitation

1. Brute Force Attacks and Password Cracking
2. Using Metasploit Framework for Exploitation
3. Privilege Escalation Techniques
4. Exploitation of System Vulnerabilities
5. Hash Dumping and Credential Extraction

Module 06- Network-Based Exploitation

1. Network Service Exploitation
2. Man-in-the-Middle (MITM) Attacks
3. ARP Spoofing and Packet Manipulation
4. Exploiting Protocol Vulnerabilities

Module 07- Post-Exploitation

1. Data Exfiltration Techniques
2. Clearing Logs and Covering Tracks
3. Persistent Access Methods

Module 08- Web Application Basics

1. Understanding HTTP Protocols
2. Cookie Management and Sessions
3. Introduction to Web Servers and Technologies

Module 09- Web Application Reconnaissance

1. Directory and File Enumeration
2. Hidden Parameter and Resource Discovery
3. Brute Force Techniques for Login Pages
4. Subdomain Enumeration
5. Technology Profiling

Module 10- Web Application Exploitation

1. OWASP Top 10 Vulnerabilities
2. SQL Injection, XSS, and File Upload Exploits
3. Authentication Bypass and Broken Access Control

Module 11- Reporting and Documentation

1. Writing Effective Penetration Test Reports
2. Recommendations for Mitigation
3. Ethical Practices in Penetration Testing