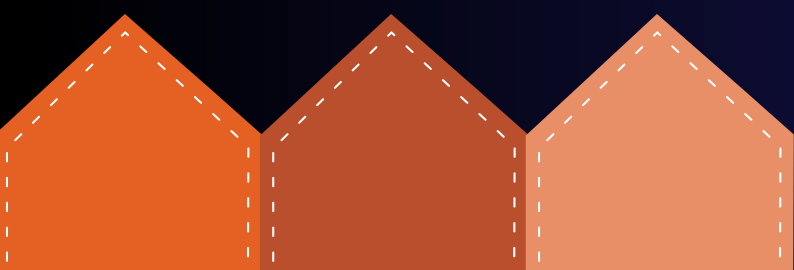
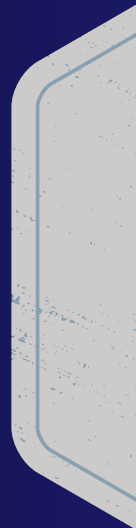




OFFENSIVE SECURITY

OSCP+

Online Training



INTRODUCTION

The OSCP+ (Offensive Security Certified Professional Plus) course is an advanced-level cybersecurity training program designed for individuals looking to take their penetration testing skills to the next level. As a highly regarded certification, the OSCP+ is tailored for those who have a foundational understanding of ethical hacking and want to deepen their knowledge in offensive security. This course will help you gain mastery in real-world penetration testing, vulnerability assessment, and exploitation techniques.

The OSCP+ focuses on providing hands-on experience with a variety of tools, tactics, and methodologies used in penetration testing, preparing learners for complex environments. The training program spans essential topics like network exploitation, privilege escalation, web application hacking, and post-exploitation techniques. It emphasizes the application of practical skills over theoretical knowledge, ensuring that participants are equipped to face real-world cybersecurity challenges.

Upon completing the OSCP+ course, individuals will be able to confidently:

- Conduct penetration testing on various systems, applications, and networks.
- Identify and exploit vulnerabilities in a structured and methodical manner.
- Appear for the OSCP+ exam and clear it.
- Apply advanced techniques in web application penetration testing, network exploitation, and post-exploitation.
- Utilize a range of tools such as Metasploit, Burp Suite, and custom scripts to perform thorough security assessments.

The course is ideal for cybersecurity professionals aiming for higher-tier penetration testing roles or anyone interested in advancing their offensive security expertise to match the demands of today's ever-evolving cybersecurity landscape. By completing the OSCP+ certification, individuals will stand out in the competitive field of cybersecurity, demonstrating their expertise and readiness for the most challenging security engagements.

OVERVIEW OF OSCP+ EXAM

The OSCP+ exam is a practical, hands-on certification designed for individuals who want to demonstrate their proficiency in penetration testing. It tests your ability to perform real-world attacks and compromises against machines and systems in a controlled, exam environment. The exam consists of a series of penetration testing challenges, testing skills related to information gathering, vulnerability analysis, exploitation, post-exploitation, and reporting.

The OSCP+ exam has a time limit of 48 hours, during which you need to complete the tasks and submit a comprehensive report detailing the attacks you performed, vulnerabilities you exploited, and how you achieved the objectives set in the exam. The exam is divided into multiple sections, each testing different aspects of the penetration testing process.

The exam is designed for experienced penetration testers and cybersecurity professionals looking to advance their skills and get certified at a higher level of expertise. Achieving the OSCP+ certification not only demonstrates hands-on technical capabilities but also prepares individuals for various security roles such as penetration testers, red team members, or security consultants. The certification is recognized in the cybersecurity industry and can significantly enhance career prospects by showcasing advanced technical skills in ethical hacking.

Course duration- 100 Hours



OSCP+ SYLLABUS

Module 01-: Introduction to OSCP Course

1. Overview of OSCP objectives and requirements.
2. Setting up a Kali Linux VM and necessary tools.
3. Introduction to PEN-200 modules and learning pathways.
4. Broad overview of penetration testing fundamentals.

Module 02- Report Writing

1. Basics of note-taking during penetration tests.
2. Tools and techniques for effective documentation (screenshot utilities, note-taking apps).
3. Structure of penetration testing documentation:
 - a. Executive Summary.
 - b. Technical Summary.
4. Writing actionable technical findings and recommendations.

Module 03- The Penetration Testing Lifecycle

1. Phases of penetration testing:
 - a. Reconnaissance.
 - b. Scanning and Vulnerability Assessment.
 - c. Exploitation.
 - d. Post-Exploitation.
2. Real-world workflow for assessments.

Module 04- Information Gathering

1. **Passive vs. active reconnaissance techniques.**
2. **Introduction to OSINT (Open Source Intelligence).**
3. **DNS, SMB, SNMP, and Web Enumeration.**
4. **Tools: Nmap, Rustscan, and custom scripts.**

Module 05-Vulnerability Scanning

1. **Understanding the vulnerability scanning process.**
2. **Installing and configuring Nessus.**
3. **Utilizing Nmap NSE scripts for vulnerability assessment.**
4. **Interpreting scan results for actionable insights.**

Module 06- Introduction to Web Applications

1. **Overview of OWASP Top 10 vulnerabilities.**
2. **Use of Burp Suite and other proxies for analysis.**
3. **Techniques to enumerate headers, cookies, and source code.**

Module 07-Cross-Site Scripting (XSS)

1. **Types of XSS vulnerabilities: Reflected, Stored, DOM-based.**
2. **Exploiting XSS for privilege escalation.**

Module 08- Directory Traversal

1. Absolute vs. relative paths in exploitation.
2. Encoding techniques for bypassing filters.

Module 09- File Inclusion Vulnerabilities

1. LFI vs. RFI attacks.
2. Using PHP wrappers and other advanced techniques.

Module 10- File Upload Vulnerabilities

1. Identifying and exploiting file upload flaws.
2. Bypassing content-type validation.

Module 11- Command Injection Vulnerabilities

1. Basics of OS command injection.
2. Chaining commands to gain access.

Module 12- SQL Injection Vulnerabilities

1. Advanced SQL injection types: Error-based, UNION-based, Blind SQLi.
2. Exploiting MSSQL databases with xp_cmdshell.
3. Automation using SQLMap.

Module 13- Attacks on Client-Side Applications

- 1. Preparing for Office document attacks using macros.**
- 2. Leveraging Windows shortcuts and library files.**

Module 14- Public Exploits (Online and Offline)

- 1. Reviewing online exploit repositories.**
- 2. Using SearchSploit and frameworks for offline exploitation.**

Module 15- : Exploit Adaptation and Development

- 1. Basics of Python Programming.**
- 2. Debugging and upgrading existing exploits.**

Module 16- Antivirus Evasion

- 1. Understanding AV detection methods.**
- 2. Manual and automated AV bypass techniques.**

Module 17- : Password Attacks

- 1. Brute-forcing SSH, RDP, and HTTP logins.**
- 2. NTLM hash cracking and pass-the-hash attacks.**

Module 18- Windows Privilege Escalation

1. Enumerating sensitive information using tools like PowerShell.
2. Techniques: DLL hijacking, unquoted paths, and Scheduled Tasks.

Module 19-: Linux Privilege Escalation

1. Exploiting misconfigured cron jobs, SUID binaries, and kernel vulnerabilities.
2. Utilizing special sudo permissions.

Module 20-: Port Redirection and SSH Tunneling

1. Techniques for port forwarding using Socat and SSH.
2. Local, remote, and dynamic forwarding.

Module 21- Advanced Tunneling

1. HTTP and DNS tunneling using tools like Chisel and dnscat.



Module 22- Metasploit Framework

1. Exploiting vulnerabilities using Metasploit modules.
2. Post-exploitation and pivoting techniques.

Module 23- Introduction and Enumeration

1. Active Directory enumeration using tools like BloodHound.
2. Gathering domain-specific data for further exploitation.

Module 24- Attacking AD Authentication

1. Techniques like Kerberoasting and NTLM attacks.
2. Exploiting SPN-based vulnerabilities.

Module 25- Lateral Movement in AD

1. WMI, WinRM, and Pass the Hash techniques.
2. Persistence using golden tickets and shadow copies.



Module 26- Assembling the Pieces

1. Practice labs simulating full pentesting workflows.
2. End-to-end attack scenarios:
 - a. Reconnaissance to exploitation.
 - b. Privilege escalation to report writing.

Module 27- Reporting and Presentation

1. Presenting findings in a professional format.
2. Emphasizing actionable recommendations.

Note: Please confirm payment details via our official WhatsApp  +91-9318492128 before making any payment. Ensure the Payment Account name is 'CyberiumX' only.

CYBERIUMX