"Offensive Security OSCP Certification: 10-Day Intensive Prep Course"

Course Introduction:

The "PEN-200: OffSec Certified Professional (OSCP) Exam Prep" is an intensive 10-day course designed to prepare learners for the OSCP certification exam. This course emphasizes hands-on technical skills, critical thinking, and real-world penetration testing methodologies. Each day focuses on specific areas necessary for building a robust foundation in offensive security, ensuring learners can tackle the challenges of the exam and practical scenarios in the field.

Day 1: Introduction to Penetration Testing

• Understanding the Penetration Testing Life Cycle: Explore the stages of reconnaissance, scanning, exploitation, and post-exploitation.

• Setting Up the Lab Environment: Guidance on configuring a virtual lab for practical exercises.

• Introduction to Offensive Security Mindset: Develop the mindset required for effective penetration testing.

Day 2: Information Gathering

• Passive Information Gathering: Learn techniques for collecting data without interacting with the target systems.

• Active Information Gathering: Explore methods that involve direct interaction with a target.

• Tools for Recon and Enumeration: Introduction to essential tools like Nmap and Wireshark.

Day 3: Vulnerability Scanning

• Understanding Vulnerability Scans: Learn the purpose and methodology behind scanning for vulnerabilities.

• Automated vs. Manual Scanning: Discuss the advantages and limitations of both approaches.

• Using Vulnerability Scanners: Hands-on practice with tools like Nessus and OpenVAS.

Day 4: Gaining Access

• Exploitation Basics: Understand the principles behind exploiting vulnerabilities.

• Introduction to Metasploit Framework: Familiarize with this powerful exploitation tool.

• Manual Exploitation Techniques: Explore scenarios where manual exploitation is necessary.

Day 5: Privilege Escalation

• Windows Privilege Escalation Techniques: Learn to identify and exploit privilege escalation opportunities in Windows.

• Linux Privilege Escalation Techniques: Discover methods for escalating privileges in Linux environments.

• Post-Exploitation Concepts: Discuss maintaining access and covering tracks after exploitation.

Day 6: Buffer Overflows

• Understanding Buffer Overflows: A deep dive into the concept and importance of buffer overflows.

• Writing Simple Buffer Overflow Exploits: Practice crafting basic exploits step-by-step.

• Exploiting Real-World Applications: Apply knowledge to exploit vulnerable applications.

Day 7: Web Application Attacks

• Introduction to Web Application Security: Understand common web vulnerabilities and attack vectors.

• SQL Injection and Cross-Site Scripting (XSS): Learn about these prevalent web application vulnerabilities.

• Using Burp Suite for Testing: Hands-on experience with this essential web application security tool.

Day 8: Password Attacks

• Cracking Passwords with John the Ripper and Hashcat: Explore the use of these tools for password cracking.

• Understanding Rainbow Tables: Learn how precomputed tables can expedite the password cracking process.

• Implementing Effective Password Policies: Discuss strategies for strengthening password security.

Day 9: Wireless Attacks

• Fundamentals of Wireless Security: An overview of wireless network vulnerabilities.

• Cracking WEP and WPA/WPA2: Techniques for breaking widely used wireless encryption protocols.

• Introduction to Aircrack-ng Suite: Practice using this suite of tools for wireless network penetration testing.

Day 10: Exam Preparation and Practice

• Simulating the OSCP Exam Environment: Tips on setting up a practice environment that mirrors the exam.

• Time Management Strategies for the OSCP Exam: Learn techniques to efficiently manage time during the exam.

• Reviewing Common Pitfalls and Challenges: Discuss frequent challenges faced by test-takers and strategies to overcome them.

Conclusion:

This 10-day course provides a structured path to mastering the skills necessary for the OSCP certification. Through a combination of theoretical understanding and practical application, learners will be well-prepared to tackle both the exam and real-world penetration testing scenarios with confidence.