

Module Title : Licensed Penetration Tester (Master) Training

Duration : 5 days

About the Program

The LPT (Master) is the world's first fully online, remotely proctored LPT (Master) practical exam, which challenges the candidates through a grueling 18 hours of performance based, hands-on exam categorized into three practical exams for six-hour duration each, which will test your perseverance and focus by forcing you to outdo yourself with each new challenge. The exam requires the candidates to demonstrate a methodical approach to test and validate security defenses. The LPT (Master) exam is developed with close collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

Course Outline

Module 01 Introduction to Vulnerability Assessment and Penetration Testing

Module 02 Information Gathering Methodology

Module 03 Scanning and Enumeration

Module 04 Identify Vulnerabilities

Module 05 Exploitation

Module 06 Post Exploitation

Module 07 Advanced Tips and Techniques

Module 08 Preparing a Report

Module 09 Practice Ranges

Key Elements

Real world, performance based assessment:

The successful candidates need to demonstrate a mastery of the skills required to conduct a full black box penetration test that simulates a complex network of a multi-national organization in real time. The exam environment via EC-Council's cloud based cyber range, iLabs, has multiple networks with different militarized and de-militarized zones. You will follow the entire process of "Cyber kill chain", taking you from reconnaissance, scanning, enumeration, gaining access, maintaining access, then exploiting vulnerabilities that you will have to seek out in a network that only a true penetration tester will be able to break.

Methodical Approach:

To build on the technical skills taught in the Certified Ethical Hacking course, the repeatable and documentable methodology provided in the EC Council security analyst program , the EC-Council LPT (Master) course emphasizes application of this methodical approach to penetration testing. The LPT (Master) practical exam thoroughly tests the application of the penetration testing process and lifecycle knowledge and the skills required in an examination that even our reviewers have called “extremely challenging”.

Penetration test report:

Many have described report writing as one of least preferred, yet arguably one of the most critical parts of any penetration testing engagement. While so many cyber security courses are offered globally to cover various subjects in the penetration testing realm, hardly any are dedicated to this very important skill, especially almost since half of all time spent at any penetration testing engagement can revolve around writing and reporting the core findings of the engagement to the client.

The key skill also lies in communicating a highly technical finding in an elaborate penetration test engagement to someone to the senior management and the board of directors can be very challenging and frustrating at times. Mastery of communication, research and report writing is required to make sense of technically complex topics like specific vulnerabilities and their resulting exploits in a meaningful manner to make educated decisions to improve the security posture of the organization. The candidates are required to submit a comprehensive report of their findings, methodology used, corroborative screenshots, scripts, custom exploits, or any other method they have used to penetrate the network within 45 days after completing the three challenges. The submitted report should be very clear, so that we should be able to compromise the target again by following the report.

Remote Proctoring

EC-Council launches the first ever remotely proctored online Pen-Testing Exam as a mechanism to ensure the authenticity of the test taker. This not only adds credibility to the overall title but also eliminates external influences that can change the exam outcome. While this test does not limit the test taker to explore his research skills and take advantage of documented resources available, it keeps a check on the individual capability of dealing with the challenges by himself.

Eligibility Criteria

To be eligible to apply to sit for the LPT (Master) Exam, candidate must either.

- Hold an ECSA / ECSA (Practical) or LPT certification in good standing (Your USD100 application fee will be waived);



Course Outline :: Licensed Penetration Tester (Master) Training::

- or Have a minimum of 2 years working experience in pentesting (You will need to pay USD100 as a non-refundable application fee);
- or Have any other approved industry certifications such as OSCP or GPEN cert (You will need to pay USD100 as a non-refundable application fee)