EC-Council

LPT LICENSED PENETRATION TESTER MASTER

Advanced Penetration Testing

The Ultimate Penetration Testing Standard

COURSE DESCRIPTION

ADVANCED PENETRATION TESTING

The Advanced Penetration Testing program is created as a progression for ECSA credential professionals.

The course is designed to show the advanced concepts of scanning against defenses, pivoting between networks, deploying proxy chains and using web shells. The “virtual cyber ranges” bring practicality into the training sessions and are designed to provide hands on skills that demonstrates how professional pentesters determine the attack surface of targets within a required time frame and gain access to the machines and escalate privileges.

The practical environment ranges progress in difficulty and reflect enterprise network architecture. This environment includes defenses and challenges which candidates of the LPT program must defeat and overcome. This is not done through a typical FLAT network! As candidates progress through the various range levels, each encounter will present the top defenses of today and they will learn the latest best practices, tips and tricks, and even evasion techniques.

EC-Council brings to you a new range of real world challenges that will not only test your Pen-testing skills but guarantees you an experience that is not built for the weak hearted. If you have been looking for a way to test your Pen-testing abilities, this is your chance to prove you have what it takes.

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

Licensed Penetration Tester (Master)

The LPT (Master) is a fully online, remotely proctored, practical exam, It is categorized into three practical exams of 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.

LPT (Master) certified professionals can:

Demonstrate a repeatable and measurable approach to Penetration Testing

Perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS), LFI, RFI vulnerabilities in web applications

Get access to proprietary EC-Council Penetration Testing methodologies

Exploit vulnerabilities in Operating systems such as Windows, Linux

Perform privilege escalation to gain root access to a system Demonstrate 'Out-of-the-box' and 'lateral' thinking

Identify and bypass perimeter protections	In an enterprise network their will be protections, you will learn how to identify the protections in place and bypass them to extract the data even when protected with IPS and endpoint protections

Perl, Python and Ruby scripting for the penetration tester	As a practitioner you have to be able to modify and change the methods of attacking an enterprise network, this requires custom scripting to defeat signature and anomaly based protection mechanisms
Advanced post exploitation and persistence	Gaining access is a small part of a professional penetration test, once you have the access, the ability to move laterally, and exfiltrate the data from the enterprise requires post exploitation skills
Extending Metasploit with custom modules and exploits	To use open source code in a penetration test requires knowledge of the modules, and the ability to customize them based on the data you have obtained from the targets
Pivoting from external into internal networks	Virtually all enterprise networks have external facing machines as well as internal intranet machines, the preferred way to access these is through pivoting and using the initial source of access to leverage your way into the enterprise intranet
Avoiding the most common mistakes when drafting a professional penetration testing report	Having skills is one thing, but being able to provide tangible findings to the enterprise client is critical for a professional penetration tester

Elements that make LPT (Master) one of a kind

Strictly designed for real life Penetration Testers:

The LPT (Master) exam mimics a real life enterprise network with multiple network segments, firewalls, Demilitarized Zones (DMZ), varied operating systems, different web technologies, access control policies, and layers of security controls by putting your Penetration Testing skills to test. The cyber range has no specific boundaries and forces you to demonstrate your skills across reconnaissance, scanning, enumeration, gaining access, maintaining access, then exploiting vulnerabilities and seeking out into a network that only a true professional will be able to break.

Built by the best:

The scenarios witnessed by the candidate during the exam are outcomes of real life experiences that are put together by the best in the business; the exam development cell involves SMEs and practitioners who bring in real world Penetration Testing capabilities to achieve consistent results.

Leverage Industry Standard Methodologies:

The LPT (Master) methodology builds on the available open-source penetration testing methodologies, e.g. - PTES, NIST800-115, PCI DSS, ISSAF, OSSTMM and many others. Some of these methodologies are (industry) vertical specific while others tend to cover broader practices. The LPT (Master) certification blends best of breed industry methodology while challenging you to go deeper into the technical aspects of penetration testing.

We Spoke To Our Customers

Critical Testing Design Ingredients:

Progressive assessment patterns:

Studies prove that progressive assessment patterns produce higher reliable results as compared to traditional assessment patterns. The LPT (Master) certification exam is designed as real-world scenario in a progressive 3 level challenge that includes defensive and offensive challenges which you must defeat and overcome. This is not the typical FLAT network! As the candidate progresses through the levels, it challenges the candidates' knowledge, skill and ability of compromising different systems while leveraging on advanced evasion techniques.

Time-bounded gamified design

The reality and essence of a real time penetration testing experience is a blend of time and stress constraints. A number of psychology studies show that time bounded tests with a gamified design (vs an open-ended test without simulation) can bring about higher levels of influences on performance, resulting in invalid outcomes. The LPT (Master) challenges are designed to push candidates to perform under time pressure, requiring a demonstration of higher level of skill as candidates move through different difficult levels of the exam.

Deep-dive analytical approach:

If you think you can "wing it", think again. The LPT (Master) challenges are designed to test your skills on key aspects of penetration testing at various intervals, each in a different scenario. There is no way to memorize the answers or "wing it". This process ensures that you have the required analytical eye to capture important data and use this to proceed towards the end goal of completing the task. With this, we will be able to certify your skills of being able to exploit vulnerabilities as a world class penetration tester.

Virtual Lab Environment:

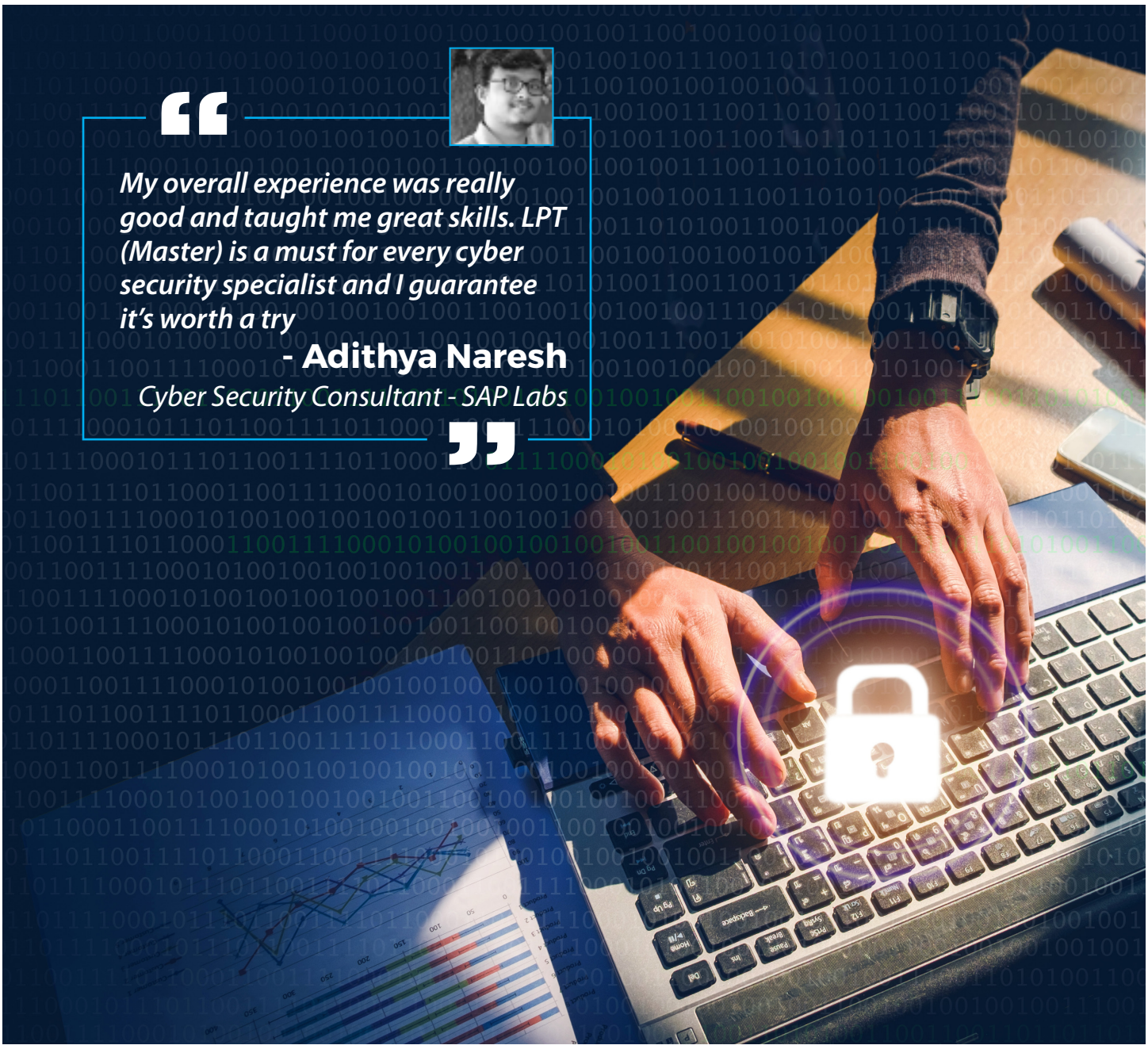
EC-Council will provide the entire cyber-range through its cloud based cyber range, iLabs. The LPT (Master) labs are designed to give the user the ultimate hands-on experience. Each exercise category has its own Virtual Private Cloud that comes preconfigured with vulnerable websites, Victim Machines, and the environment is LOADED with tools. This also includes all the supporting tools required to explore and launch your attacks.

Remote Live Proctoring:

EC-Council launches the world's first remotely proctored, online penetration testing exam as a critical industry requirement to verify the identity of candidates while providing a controlled environment to protect the sanctity of such a high stake exams. This process ensures the credibility to the LPT (Master) credential by eliminating external influences that can affect exam results. While this exam does not limit the candidate to leverage their research skills and take advantage of documented resources available, the proctored exam maintains a close monitoring of the exam session to ensure complete compliance to examination requirements.

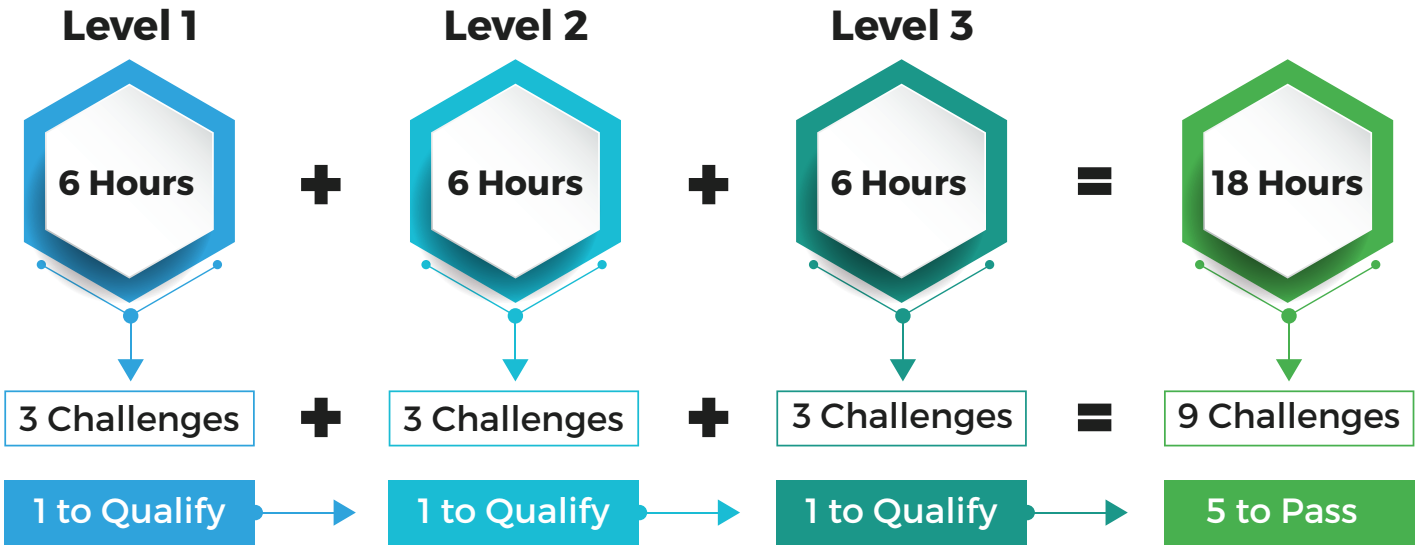
Report Writing:

To successfully earn the LPT (Master) credential, candidates are expected to fully document their Penetration Test outcomes in a professional Penetration Test report. This is an important requirement as many Penetration Testers are unable to prepare professional reports to management or clients hence reducing drastically the value of the Penetration Test exercise, since the outcomes and proposed remediation are not properly documented and communicated. The report will be reviewed and scored by an assessment rubric built by subject matter experts in the Penetration Testing domain.



Attaining Industry Trusted and Preferred Credentials LPT (Master)

The Exam



Who can take the LPT (Master) exam?

To be eligible to apply to attempt the LPT (Master) Exam, candidate must either:

- Be an **ECSA** member in good standing (Your USD100 application fee will be waived);
- Or, Attend the **Advanced Penetration Testing** course.
- Or, possess a minimum of **2 years** of Penetration Testing work experience in Penetration Testing (You will need to pay USD100 as a non-refundable application fee);
- Or, possess any other industry equivalent certifications such as OSCP or GPEN cert (You will need to pay USD100 as a non-refundable application fee).

Recommended For:

- Penetration Testers
- Information Security Engineers
- Network Administrators
- Security Consultants
- IT Auditors

For more information on:

Application process

Renewal Cycle, Certification Fees & ECE Scheme

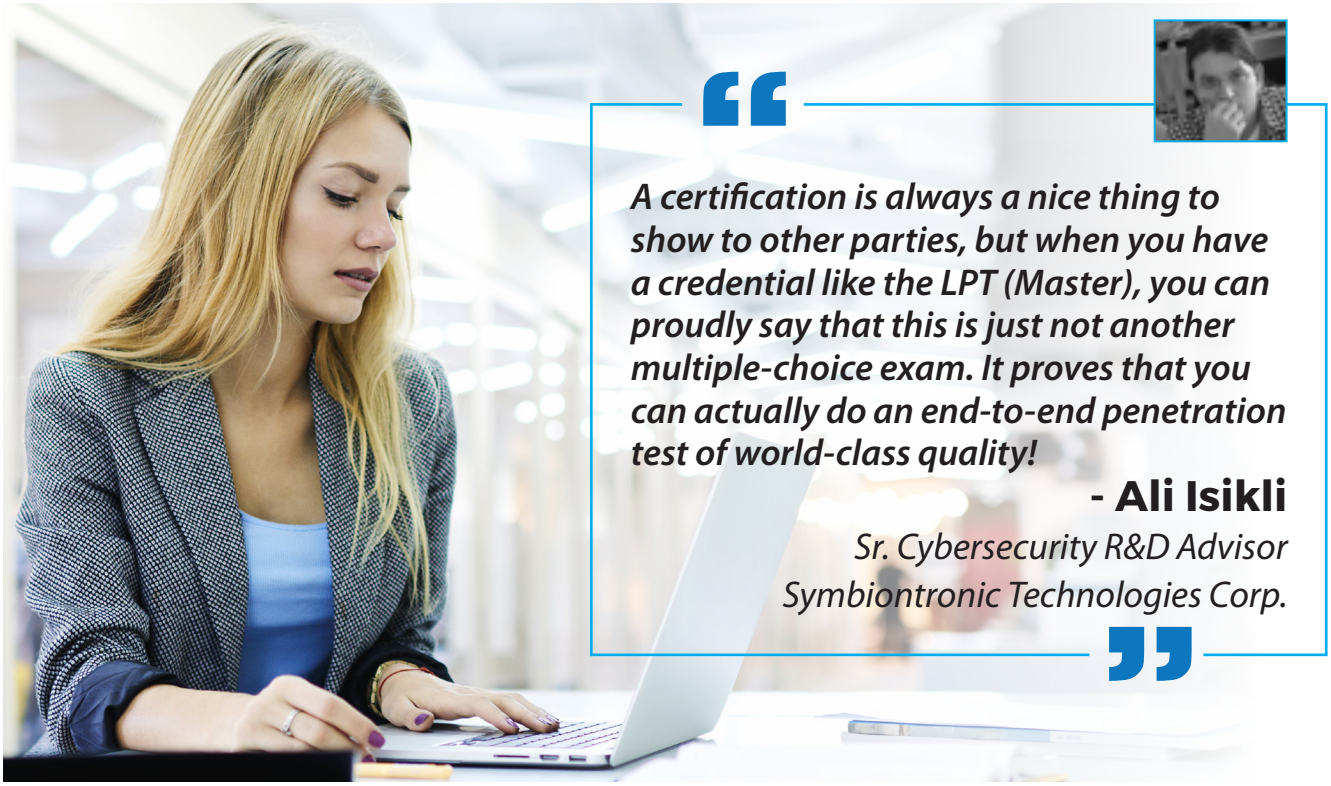
How is the exam conducted?

Please visit lptmaster.com

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);
- 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)



LPT (Master) Credential

1. Successful candidates will receive the LPT (Master) Welcome Kit consisting of:

Membership card

Printed Certificate

LPT (Master) Plaque

Welcome Letter

Lapel Pin

EC-Council LPT (Master) T-shirt

2. The LPT (Master) license is valid for 2 years. After the initial 2 years, members will have to renew their LPT (Master) license by remitting the annual USD250 renewal fee.

3. Members are required to fulfil their ECE requirements to remain in good standing.

EC-Council

www.eccouncil.org