



Licensed Penetration Tester (Master)

The Ultimate Penetration Testing Certification



About the Certification



LPT (Master) Exam

There are good penetration testers and then there are great penetration testers.

Unless you are bent on being nothing other than the best in penetration testing, don't bother registering for this program, as you are probably not cut out for it.

You will be required to make knowledgeable decisions under immense pressure at critical stages while selecting your approach and exploits.

As you progress along these levels, you will need to maneuver web application, network, and host penetration testing tools and tricks in an internal and external context to ultimately pwn the hosts and exfiltrate data required for the completion of the challenges.

Demonstrate the Mastery of Advanced Pen Testing Concepts and Techniques Including:

- | | |
|---------------------------------------|-------------------------------------|
| ■ Multi-level Pivoting | ■ Privilege Escalation |
| ■ OS Vulnerabilities Exploitation | ■ RFI/LFI |
| ■ SQL Injection | ■ Exploit and Payload Customization |
| ■ Host-Based Application Exploitation | ■ SSH Tunnelling |

You will be facing the ticking clock and there's no time to hesitate. There's no time for second-guessing. Try either of these and be prepared to fail!



Introducing the World's Most Advanced Penetration Testing Program

The Advanced Penetration Testing Course by EC-Council was created as the progression after the ECSA (Practical) to prepare those that want to challenge the Licensed Penetration Tester (Master) certification and be recognized as elite penetration testing professionals. Our training has been designed by the best in the industry and meant to push you to develop the kind of skill that you've been waiting to acquire.

LPT (Master) training is not comfortable (and the exam is even worse!) , but filled with intense stress meant to illicit the best from you. Those who prevail will have developed an instinctual and intellectual response to real world penetration testing challenges.

We want to bring out the best in you. Our aim is to push you to your limit while making you solve complex problems that actual penetration testers solve daily in the real world. For four punishing and long days, you will have to perform various tasks until it becomes second nature. This is the foundation of the program.

This program is radically different from the ECSA. In the ECSA course, you are provided guidance on what machines to attack and an initial starting point. In the Advanced Penetration Testing Course, you are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide you with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

In this course you will learn professional security and penetration testing skills. The course is designed to show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells. The last module of the course includes an SOW for each of the various networks we have created for the course. This, combined with the composition of various ranges, mimics a professional penetration test. Time is limited and you will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

In summary, only those who possess the burning desire to succeed will make it.

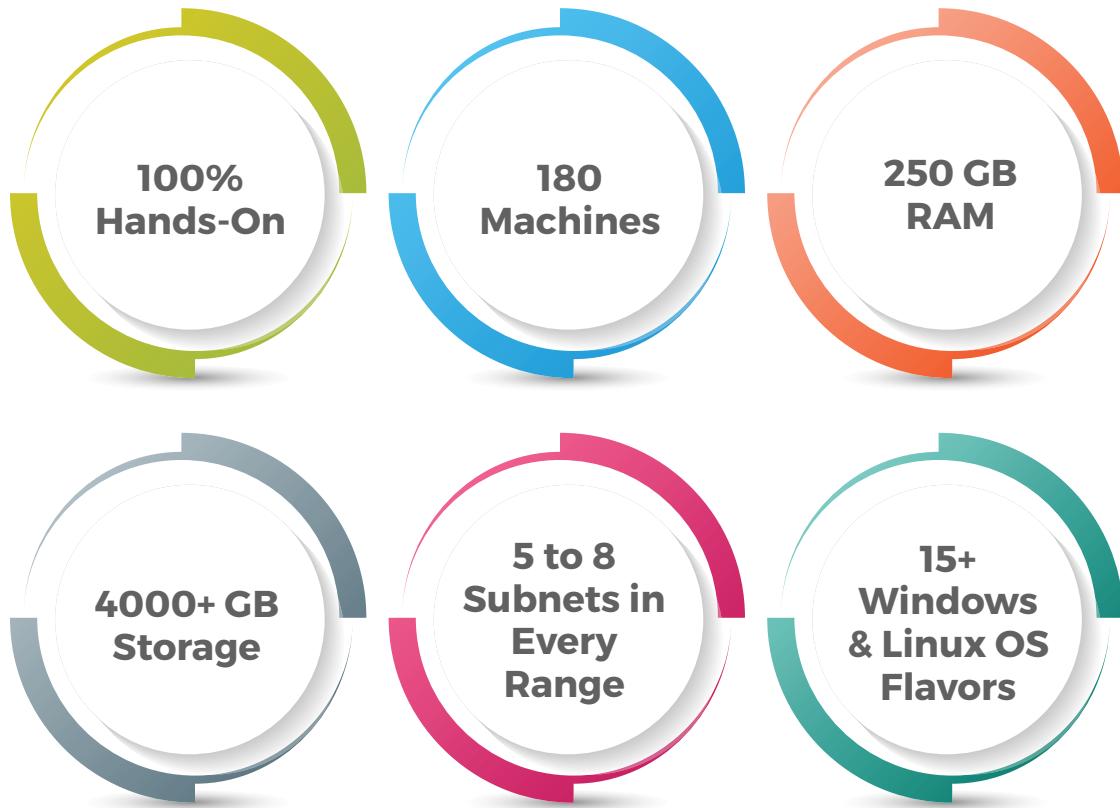


Licensed Penetration Tester (Master)

The Planet's Most Advanced Penetration Testing Range

The Advanced Penetration Testing course from EC-Council is built on the backbone of the **EC-Council's Advanced Penetration Testing Cyber Range** (ECCAPT) and this was **designed by experts** who each have more than 25 years of professional security testing across the globe.

ECCAPT: MADE OF REAL STEEL



Mimics Real-Life Pen-Testing

The range is designed to provide challenges across every level of the attack spectrum.

The ECCAPT consists of entire network segments that replicate an enterprise network — this is not a computer game simulation, this is an accurate representation of an enterprise network that will present the latest challenges

to the pen tester. Since the targets and technology continue to change, the ECCAPT is dynamic and machines and defenses will be added as they are observed in the wild. Finally, the targets and segments are progressive in nature, once you get into one machine and or segment, the next one will challenge you even more.

The final range consists of challenges that will require the skills and concepts that have been covered in the course and consist of multiple visible as well as hidden subnets to prepare you for the possible challenges of the LPT (Master) range.

Finally, the ranges are designed to teach professional-level skills to identify the attack surface of targets within a required time frame and, once this has been accomplished, to gain access to the machines and escalate privileges as required. The greater the variety of targets you encounter with and without defenses, the better of a professional penetration tester you will become.

The practical environment ranges progress in difficulty and reflect real enterprise network architecture. This environment includes defenses and challenges which you must defeat and overcome.

This is not your typical flat network! As you progress through the range levels, each encounter will present the top defenses of today and you will learn the best and latest evasion techniques.

This training format has helped thousands of penetration testers globally and is proven to be effective. Everything presented in the course is through an enterprise network environment that must be attacked, exploited, evaded, and defended.



“

As a hiring manager, LPT (Master) offers more credibility than other hands on certification, as it is fully proctored

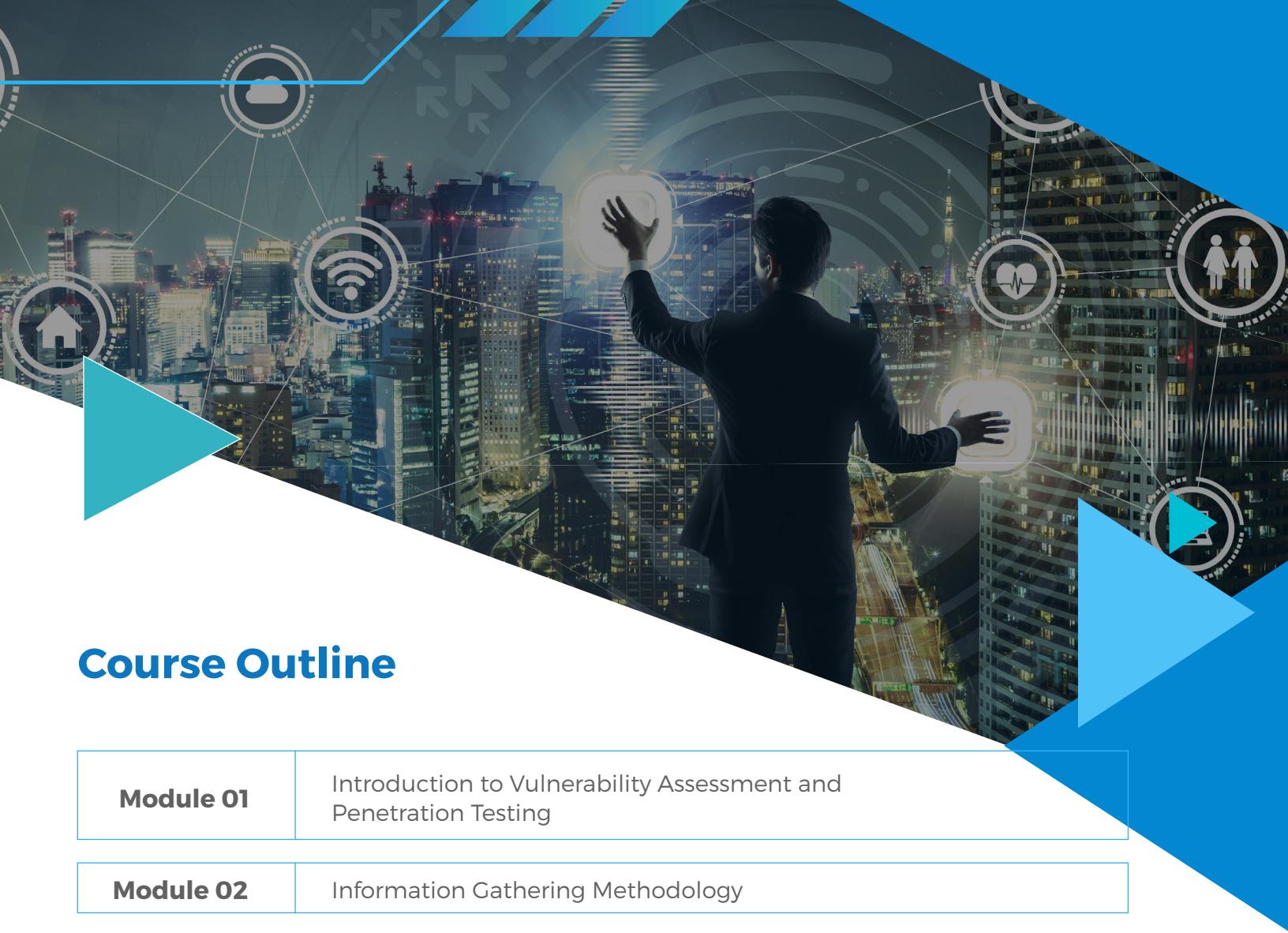
- Josh Tomkiel

Manager, Security Testing and Assessment

Schellman & Company, LLC

CCSK, OSCE, OSCP, Security+, CISSP, LPT (Master)

”



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 there 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



Licensed Penetration Tester (Master)

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.

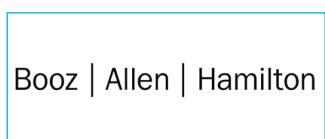
Built by the best:

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.

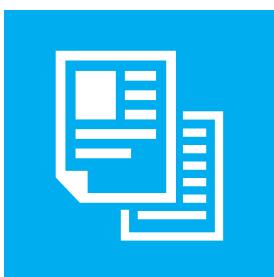
Leverage Industry Standard Methodologies:

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.



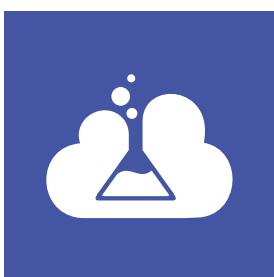
Time-bounded gamified design

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.

“My overall experience was really good and taught me great skills. LPT (Master) is a must for every cyber security specialist and I guarantee it's worth a try

- Adithya Naresh

Cyber Security Consultant - SAP Labs



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?

Eligibility Criteria

There is no predefined eligibility criteria for those interested in attempting the LPT (Master) exam. You can purchase the exam dashboard code [here](#).

Clause: Age Requirements and Policies Concerning Minors

The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.

Application Process

In order to proceed with the exam the below steps will need to be completed:

- The exam dashboard code can be purchased [here](#).
- Upon successful purchase, the candidate will be sent the exam dashboard code with instructions to schedule the exam.

Note: The exam dashboard code is valid for 3 months from date of receipt.

Should you require the exam dashboard code validity to be extended, kindly contact Ipt@eccouncil.org before the expiry date. Only valid/ active codes can be extended.



“



A certification is always a nice thing to show to other parties, but when you have a credential like the LPT (Master), you can proudly say that this is just not another multiple-choice exam. It proves that you can actually do an end-to-end penetration test of world-class quality!

- Ali Isikli

Sr. Cybersecurity R&D Advisor
Symbiontronic Technologies Corp.

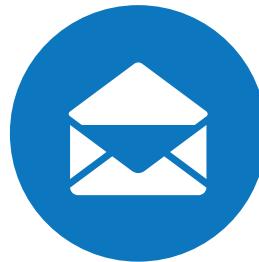
”

LPT (Master) Credential

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



Printed Certificate



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.

**This Exam Has One Purpose:
To Differentiate The Experts From The Novices In
Penetration Testing!**

EC-Council
www.eccouncil.org