EC-Council

THE ULTIMATE
PENETRATION TESTING STANDARD

LICENSED PENETRATION
TESTER (MASTER)

L|P|T
Licensed   Penetration   Tester
MASTER
™

Lack of **(professional)** Penetration Testing skills is becoming one of the biggest limitation in effectively securing organizations.
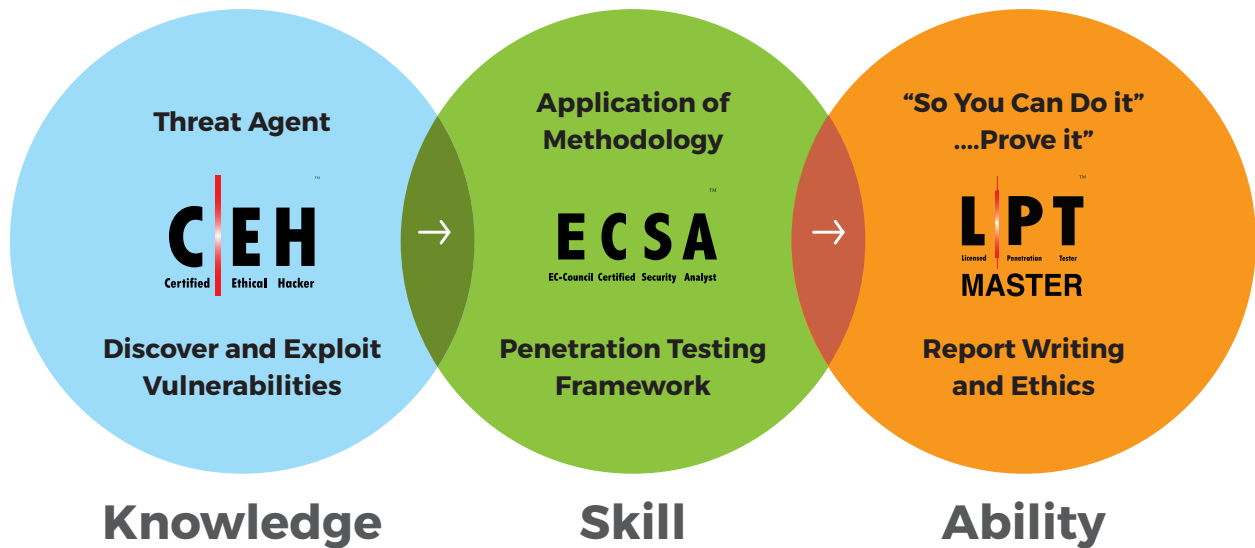
Introduction

EC-Council brings to you LPT (Master), the World's First Fully Online, Remotely Proctored Hands-on exam for Penetration Testers. If you have been looking for ways to test your Penetration Testing abilities, this is your chance to prove you have what it takes.

The exam challenges you through a gruelling multi-stage performance based scenarios mimicking a typical large networked environment. Being an LPT (Master) means that you can find chinks in the armour of defence-in-depth network security models with the help of network pivoting, making exploit codes work in your favour, or by writing Bash, Python, Perl, and Ruby scripts. This completely Hands-on exam offers a challenge like no other by simulating a complex network of a multi-national organization in real time.

The LPT (Master) is a natural evolution and extended value addition to EC-Council's series of ethical hacking and security assessment certifications. The exam is developed for next generation information security professionals in close collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

The Learning Track

Threat Agent

C|EH
Certified Ethical Hacker

Discover and Exploit Vulnerabilities

Application of Methodology

E C S A
EC-Council Certified Security Analyst

Penetration Testing Framework

"So You Can Do it" ....Prove it"

L|PT
Licensed Penetration Tester
MASTER

Report Writing and Ethics

Knowledge   Skill   Ability

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

◆ Submit a professional and industry accepted report that achieves management and technical buy-in

◆ Get access to proprietary EC-Council Penetration Testing methodologies

◆ Write exploit codes to gain access to a vulnerable system or application

◆ 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

For more information Please visit **lptmaster.com**

L|PT
MASTER

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
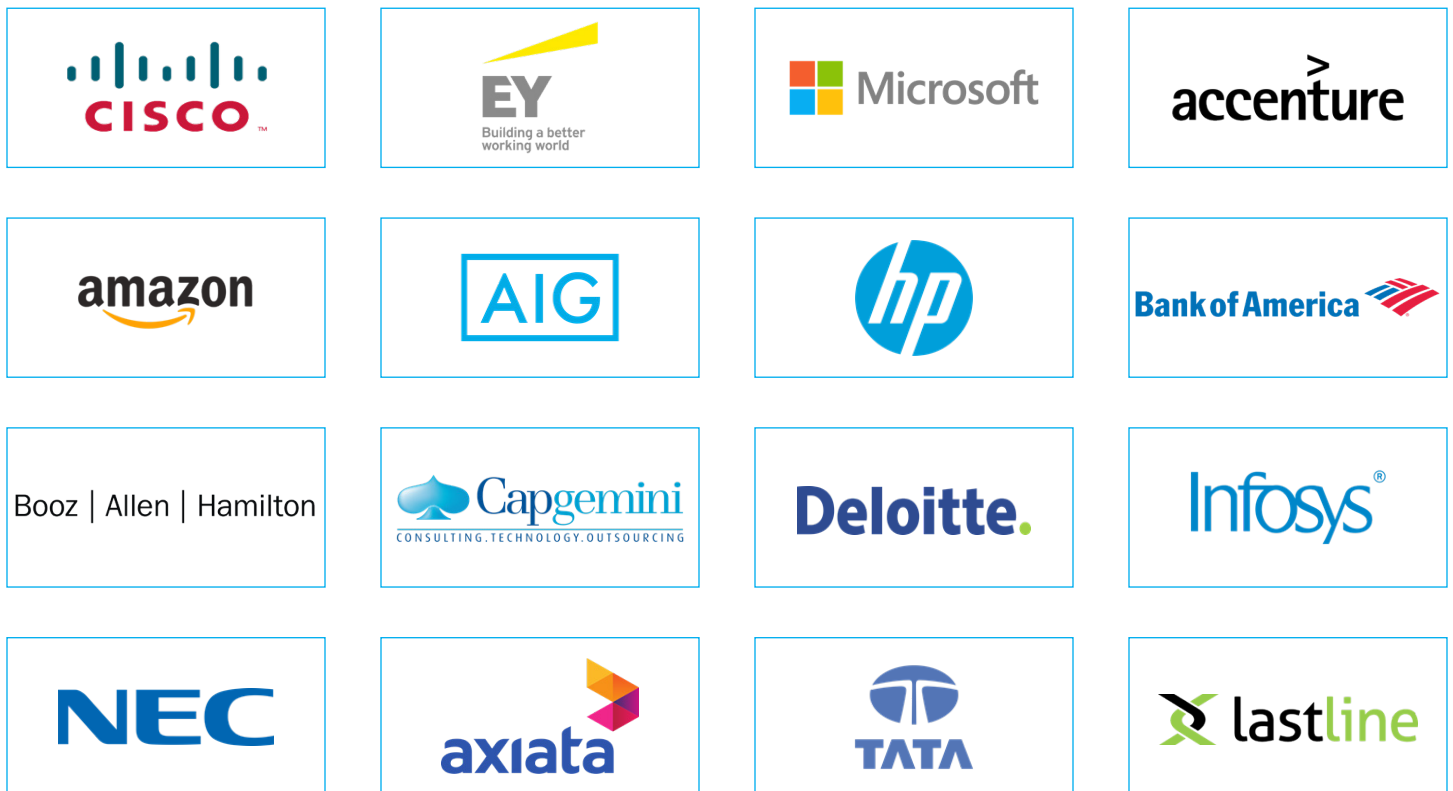
For more information Please visit **lptmaster.com**

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.
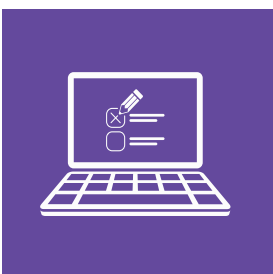
Remote Live Proctoring:

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.

LPT
MASTER

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
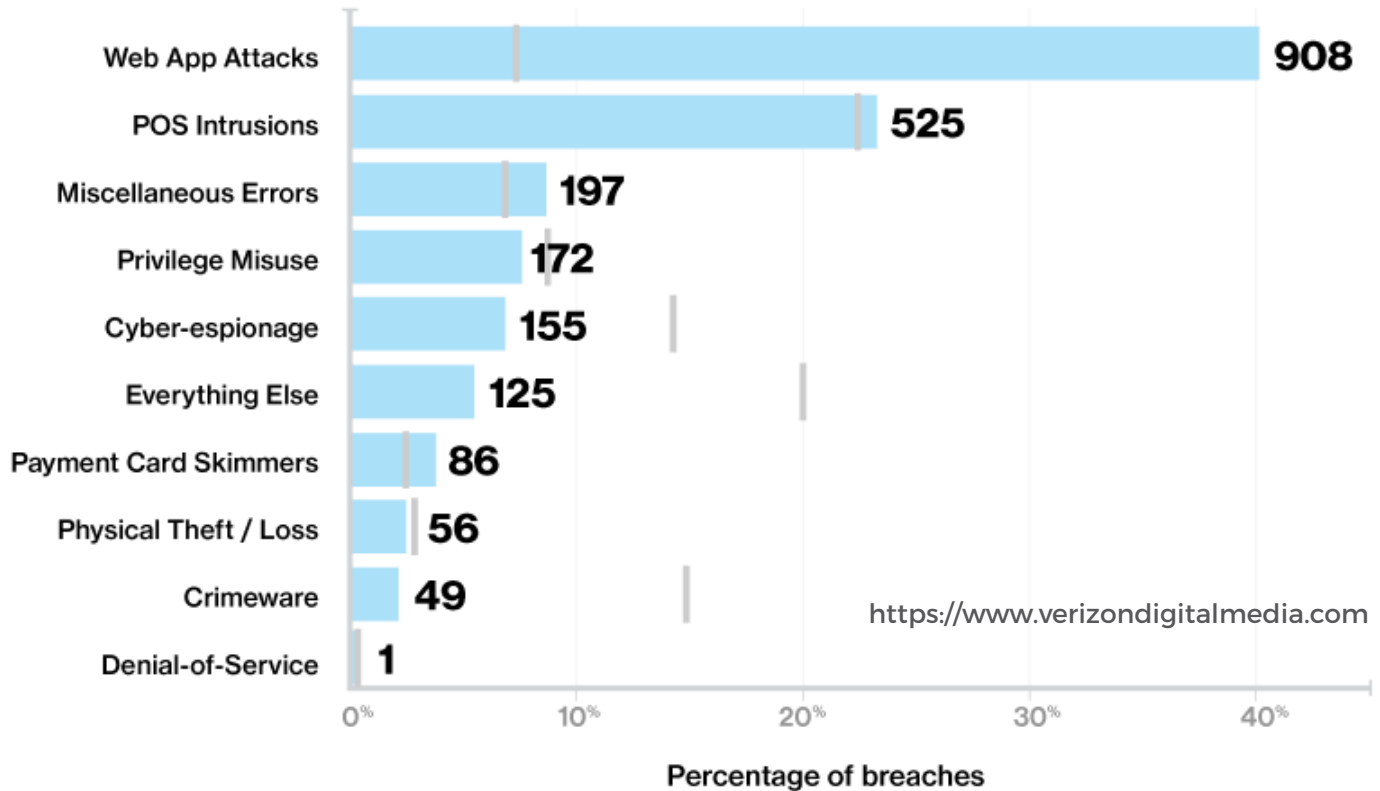
- Adithya Naresh
Cyber Security Consultant - SAP Labs

LPT (Master) Exam Challenges Represent the Current Threat Scenario

Percentage and count of attacks that resulted in data breaches per pattern, DBIR 2016

Attack Pattern	Count
Web App Attacks	908
POS Intrusions	525
Miscellaneous Errors	197
Privilege Misuse	172
Cyber-espionage	155
Everything Else	125
Payment Card Skimmers	86
Physical Theft / Loss	56
Crimeware	49
Denial-of-Service	1

Percentage of breaches (0% – 40%)

https://www.verizondigitalmedia.com

> **Percentage of data breaches that leveraged web application attacks has increased rapidly in the last year – from only about 7 percent in 2015 to 40 percent.**

Source: Verizon DBIR 2016 Report

LPT MASTER

The Exam

Level 1   **Level 2**   **Level 3**

6 Hours **+** 6 Hours **+** 6 Hours **=** 18 Hours

| 3 Challenges | **+** | 3 Challenges | **+** | 3 Challenges | **=** | 9 Challenges |

| 1 to Qualify | → | 1 to Qualify | → | 1 to Qualify | → | 5 to Pass |

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 Have a minimum of **2 years** working experience in Penetration Testing (You will need to pay USD100 as a non-refundable application fee);

✓ or Have 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 (White Hat hackers)   ✓ Information security engineers

✓ Network administrators   ✓ Security consultants

✓ IT Auditors

For more information Please visit **lptmaster.com**

LPT
Licensed Penetration Tester
MASTER

Knowledge that would help you earn the title:

✓ Advanced scanning methods	✓ Attacking from the Web
✓ Client side Penetration Testing	✓ Attacking from the LAN
✓ Breaking out of restricted environments	✓ Bypassing network-based IDS/IPS
✓ Privilege escalation	✓ Post-exploitation

For more information on:

Application process

Renewal Cycle, Certification Fees & ECE Scheme

How is the exam conducted?

Please visit lptmaster.com

> *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

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.

For more information Please visit **lptmaster.com**

EC-Council

www.eccouncil.org