

# Re: Licensed Penetration Tester LPT

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-04/msg00204.html>

---

- *From:* Pete Herzog <[lists@xxxxxxxxxx](mailto:lists@xxxxxxxxxx)>
  - *Date:* Fri, 21 Apr 2006 10:08:37 +0200
- 

Hi,

Ability really does matter and is tough to measure. But possible.

Disclaimer: I work for ISECOM. I wanted to point out that with all this talk about ability over certification, that this is exactly the problem ISECOM addresses with the OPST and OPSA. Both courses focus on the ability— applied knowledge— required for those in security testing and security analysis. Ability is such a major part of the certification that the test-taker can use books, notes, and the internet as resources during the exam. While neither the OPST nor the OPSA is specifically for penetration testing (for example it is more about recognizing and verifying a security problem than about tools or writing exploits which is something many pen-testers like to focus on) the one thing that makes it really different is that the certification does actually measure ability under time pressure. This is why it's so popular with certain industries and government institutions as a vetting tool for new hires and promotions because at the very least, they know from the exam transcript the skill strengths and weaknesses of the candidate for the basic requirements.

You can read up more on both at [www.opst.org](http://www.opst.org) and [www.opsa.org](http://www.opsa.org) if you'd like.

FYI, we've noticed some scary patterns in what areas the majority fails to be able to do correctly and what people claim to do or have experience in. Interestingly, those who label themselves working as penetration testers or ethical hackers often make the mistake of not understanding how the tools actually work (for example what type of responses are needed for the tool to function correctly and how to verify it). Or they trust their tools too much (for example labeling a system as OpenBSD because NMAP fingerprinting says it is even though all the additional information one can find about the system clearly shows it cannot be). We see this pattern in both the OPST and OPSA. This inevitably causes problems on the exam for them from the initial logistics (checking the network parameters before starting the test) and right through to verifying if a problem (vulnerability) exists or is a false positive. I can only imagine how badly they screw up real-world audits where situations can get more odd or more complex than the scenarios they may encounter in the exams.

Anyway, I really think we're not ready yet to start "licensing" professionals. However, once the average pen tester begins working in areas that affect the safety of living things both directly and indirectly, we will need to consider a form of licensed practitioner.

Sincerely,  
-pete.

James Boomer wrote:

Re: Licensed Penetration Tester LPT

I couldn't agree with you more. But if someone has the knowledge and the know how then taking the exam won't hurt a bit. But I completely agree with you 100% as I myself own a Security Consulting Firm and have run into the same problem. You need to Know the practical side and the real life side and finding good people who do and keep current on it is always a challenge.

---

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php) And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxx for details.

---