# Legaltech news

An **ALM** Publication

# A Battle Cry for Penetration Testers: Try Harder! Earn Your OSCP Certification

*The OSCP designation is redefining expectations of excellence going far beyond pure proactive cybersecurity proficiency.*
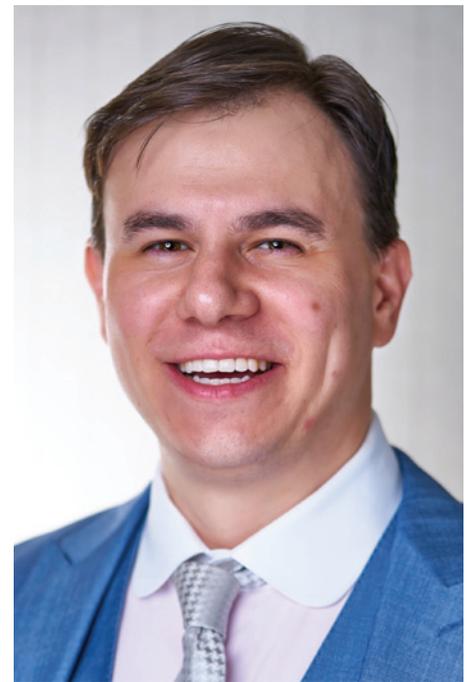
*BY JARED COSEGLIA*

In a sea of cyber certification offerings surrounded by oceans of vocational and university programs all independently creating curricula, training methodologies and proficiency validations for information security professionals and practitioners, one program is developing a reputation for being undeniably credible when it comes to the penetration testing process and life cycle: the OSCP. The OSCP (Offensive Security Certified Professional) accreditation was created and is administered by the organization Offensive Security. Its value, however, may go far beyond pure proactive cybersecurity proficiency and touch upon more ethereal characteristics about the individuals who hold one.

The OSCP exam is the self-proclaimed "world's first completely hands-on offensive information security certification." Its goal is testing and certifying an ability "to be presented with an unknown network, enumerate the targets within their scope, exploit them and clearly document their results in a penetration test report." The OSCP is 100 percent practical, contains no Q&A and no multiple choice. Sitting to take the OSCP takes 24 hours and strong internet access to connect virtually to a remote lab. Challenges presented to the test-taker are random, so everyone who sits gets a totally different experience while still measuring the same core skills. To certify you must complete the entire consecutive 24-hour exam and then write a report documenting the accomplishments within 24 hours of completing the practical. The exam is scored pass or fail. No core changes have been implemented in the exam process since the inception of the OSCP, and this approach is at the core of OSCP culture.

"We've always taken an untraditional approach to the certification process," says Jim O'Gorman, president of Offensive Security. "People are sometimes intimidated by the OSCP exam and feel they need to do a lot of prep work before signing up," admits O'Gorman, "but if you have a basic understanding of scripting, familiarity with Linux and Windows administration, you'll be fine. You'll get through the material.

Registering to take the OSCP comes with study materials tied to pen testing with Kali, coursework

**JARED COSEGLIA**

and access to a remote lab. "Take the labs seriously," implores O'Gorman. "When taking the class, it's important individuals go through the courses and do all the exercises. The simple mistakes are the ones most often made."

All the preparation and technical expertise gathered and garnered before taking the OSCP exam is only half the challenge. "The time

crunch is the hardest part of the exam," warns O'Gorman. "Twenty-four hours might seem like a long time, but realistically, it can be tight." Administrators of the OSCP are absolutely observing and monitoring the psychological choices made during the exam as much as the technical ones. O'Gorman adds, "When you eat, when you sleep, when you know to complete an item without distraction— all are core aspects of taking the exam." OSCP administrators have found that people with extreme technical depth sometimes underestimate the mental preparation necessary for the exam. The ability to identify and witness the fortitude and ability to handle stress and solve problems effectively in a time-sensitive security environment is what distinguishes the OSCP from all other proactive security certifications.

"The real value of the OSCP [preparation and exam] is that it works as a strong filter for those who are passionate, talented and have a willingness to work hard versus those that are good test takers," says O'Gorman. The creators of the OSCP have a deep appreciation for the time and effort it takes to get OSCP certified. Getting the OSCP may be time-consuming, but it is not expensive. "The cost of getting the cert comes to blood, sweat and tears and not the financial aspect of it," says O'Gorman. The initial first month of lab time and the training courses are around $800. Test retakes are only $60. Everything is virtual. "This has a high failure rate," says O'Gorman, "but that doesn't make someone a bad student or employee. The test is hard. So, we've made cost



no barrier to enable many to have access to the exam."

It is a point of pride with O'Gorman, who helped conceive the exam, that OSCP holders value more than the security knowledge they gain from the achievement. The real takeaway for many is the confidence in problem-solving and overcoming the challenges that the process presents, both in preparation and execution. "That's why you get such passion from OSCP alumni, because they are empowered and addicted to pushing through and solving complex problems," closes O'Gorman. "Those that hit the failure wall and come back … that says a lot about their tenacity."

Tenacity and passion may not be the initial variables hiring manager's use when assessing talent in the cybersecurity vertical. Right now, with an enormous talent gap of excessive demand and insufficient supply, security hiring managers may settle for the technical skills to plug-and-play people as best as possible rather than staffing on the fortitude and

zeal of the professional safeguarding their network. As more training becomes available and talent proliferates to meet the demand in the market, how hiring managers identify and validate skills in security will be challenged by the fractured diversity of available security certifications available today. The OSCP is clearly looking to differentiate not only with the substance of the certification, but also with the style. The slogan for the OSCP is "Try Harder! Earn your OSCP Certification." For OSCP holders and perhaps for hiring managers, that mantra speaks volumes about the people who have one.

*Jared Coseglia is the founder and CEO of TRU Staffing Partners, an Inc 5000 Fastest Growing American Company 2016 & 2017 and National Law Journal's #1 Legal Staffing Agency, and has over 15 years of experience representing thousands of professionals in e-discovery and cybersecurity throughout the world.*