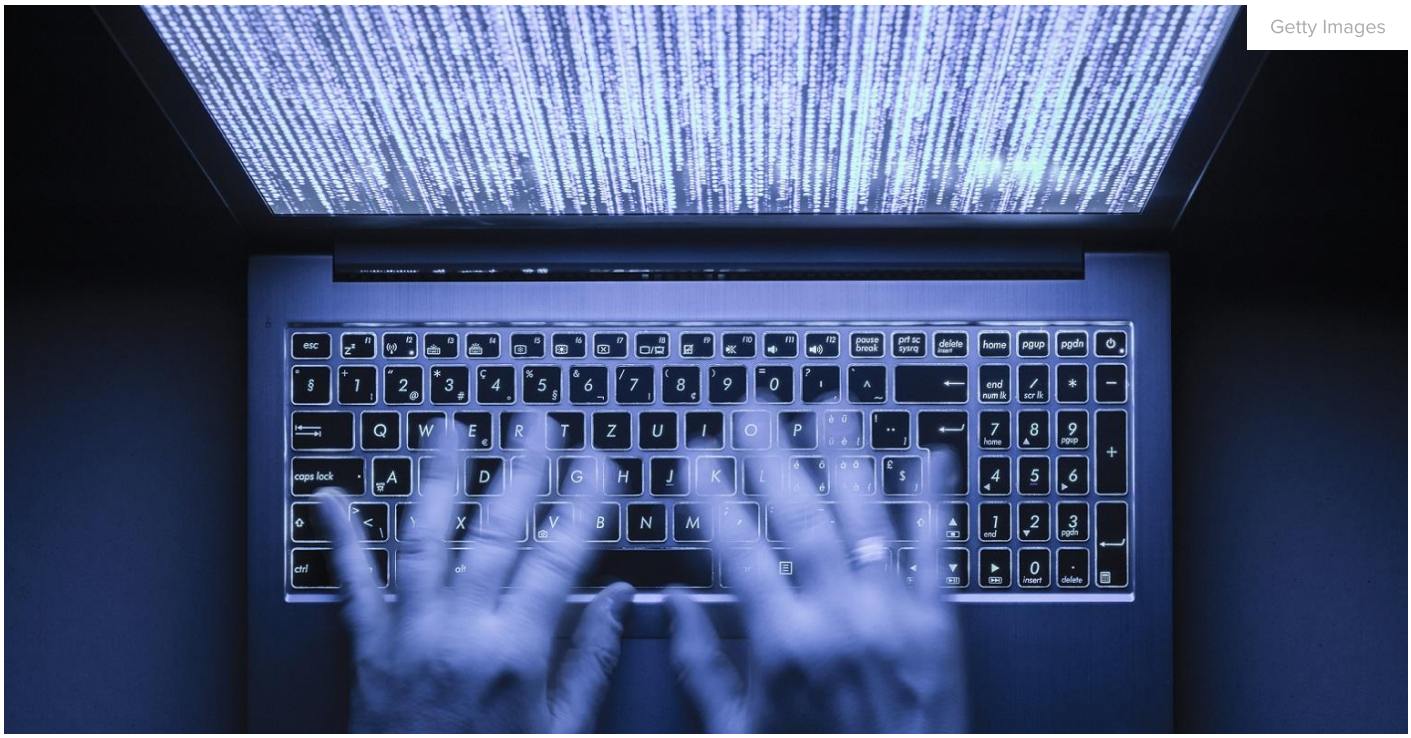

Getty Images

SECURITY > THREAT MANAGEMENT

How to Get the Most Out of Your Penetration Tests

While there are myriad benefits to conducting penetration tests, not all tests will provide the results you need. These tips will help organizations get the best value from pen testing.

Karen D. Schwartz | Jul 13, 2020

Many IT professionals and security executives agree on the value of conducting

While one of the main purposes of pen testing is to identify vulnerabilities, a pen test is different from a vulnerability scan, said Jason Nickola, senior security consultant and chief operating officer at Pulsar Security, specializing in pen testing and red teaming. Nickola also is a SANS instructor for network penetration testing and ethical hacking.

"Although they share some common elements, there is one major difference between the two: A vulnerability assessment analyzes an environment for weakness without actually taking advantage of them, while a penetration test features actual exploitation of discovered vulnerabilities."

The most important feature of a pen test is not to simply find vulnerabilities and fix them, but to better manage business risk.

"It's about prioritizing resources for addressing your most sensitive business risks, and that's more powerful than fixing flaws before the bad guys find them," explained Ed Skoudis, an instructor at SANS Institute and president of Counter Hack, a penetration testing service provider. "It's about finding vulnerabilities, figuring out the business implications of those vulnerabilities, and then fixing those you have the time and resources while making a plan to fix the rest."

While everyone agrees on the benefits of penetration testing, not all penetration tests are created equal. Here are some tips on how to get the best value from your pen tests.

Don't rush into it. Take preliminary steps to ensure security to the greatest extent possible *before* getting a pen test. "If you get a pen test without having basic cyber hygiene and undergoing a vulnerability assessment and then fixing those vulnerabilities, your pen testers will find a lot of low-hanging fruit that you should

Determine your scope. In other words, don't take on too much at once with a pen test. That means knowing *why* you need a pen test. Maybe your network was compromised or a device that wasn't properly encrypted was stolen. If your company has experienced what looks like an insider attack, for example, you may want to focus on an internal pen test with ethical hackers posing as employees or consultants. "If you have too many goals, you won't be as effective," said David Howard, a veteran pen tester currently working for a large transportation company. What's more, taking on too much might mean that the pen test takes so long that the results may no longer be relevant. "Keep it actionable with short, quick hits," Howard said. The best way to narrow the scope is understanding why. "If somebody gave up a credential, that would indicate an inside pen test. If you lost an unencrypted laptop, you would probably do an external pen test," Howard said.

Find the right pen testers. Don't focus entirely on price because you often get what you pay for. Instead, when are interviewing candidates, ask them detailed questions about their experience, what types of tools they use, what they do to keep up with what hackers are doing today and how they are contributing to the pen testing/ethical hacker community. Your goal in asking questions is to find people who are not only good with automated tools, but can think independently. "Pen testing isn't just about automation; it's about thinking like a hacker," Howard said. Candidates also should be asking *you* a lot of detailed questions about your goals, why you want a pen test and what you have done so far.

After you have chosen a pen testing company, pinpoint exactly who will be working on your pen test. "You don't want a case where some guy whose name you have heard of closes the deal with you and then somebody you have never heard of actually does the pen test," Skoudis warned. Skoudis also recommends switching pen testers or pen testing companies every once in a while to provide a fresh view.

collaborative than adversarial and keep the lines of communication open. It can also be helpful to have at least one member of the company's IT team "ride along" for the pen test.

Evaluate whether you have actually gotten a good pen test. It can be difficult to evaluate whether your pen test was as valuable as you had hoped, but there are some tangible ways to do so. First, look for a detailed methodology section in the report. The methodology section should be detailed enough so that a skilled pen tester could read it and repeat the work and have the same findings, Skoudis said. In addition, look for a discussion of the business implications of what was discovered. "They should be written with a mind toward the business implications of the finding and not only the technical/hacking implications," he said. "They could be missing the big picture if they are focused on one technical tree and missing the forest of business implications." Finally, look at how actionable the recommendations are.