hackerone

THE PEN TEST DILEMMA

3 Common Issues with Traditional Pen Tests

Rethinking Pen Tests: How Hackers Can Improve Results and ROI

Penetration tests are a staple in your security program.

But while traditional pen tests remain a useful exercise to identify potential weaknesses and strengths, they are limited in that they provide only a point-in-time view of a scope's risks. Pen tests take place for a finite time period, usually quarterly or less often, and may not capture the more timely risks presented by today's rapid software development release cycles.

Traditional Pen Tests Have Some Limitations

Pen tests are generally conducted using a combination of manual and automated tools, and generally with a small team of a few researchers. This has definite benefits, such as directing the focus of the test on specific technologies or using specific penetration methods. But the opposite reflects the test's inherent drawbacks: it is limited in scope, methods, and time. And, it hampers the usefulness of the test by limiting or avoiding any creativity in attempting to "think like a criminal". Pen tests generally use known methods to confirm that the scope is secure against those known methods.

Pen tests also begin with the assumption that the technology is secure, and the test is to validate that assumption. But that then further limits the usefulness of the test by, again, not using novel or creative methods to attempt a breach. In today's world, where current thinking is that no technology will ever be 100% secure, the more appropriate assumption is that vulnerabilities exist and they must be found.

The maturity of an organization's security apparatus also impacts the usefulness of pen test results. As Daniel Miessler explains in his "Information Security Assessment Types" primer, "Because a Penetration Test is designed to achieve one or more specific goals, they should not be commissioned by low or medium security organizations in most cases." The reasoning is that less mature organizations will be presented with generic and overly broad results since many outstanding vulnerabilities (known or unknown) will be easily found. Since pen tests assume security is already strong, according to Miessler, organizations should conduct multiple vulnerability assessments, and address all findings, before any pen tests are conducted.

So while pen tests are necessary and do serve a valuable purpose, their drawbacks must still be addressed and those gaps filled. But how?

Bring the Crowd's Creative Wisdom

Hacker-powered security is a proven method for identifying vulnerabilities quickly, efficiently, and at a low overall cost. White-hat hackers provide continuous security, organizations pay only for found and validated vulnerabilities, and hackers bring nearly unlimited diversity of skills, approaches, experience, and desired compensation. In other words, organizations get an army of researchers eager to uncover and report bugs of all types and severities. It's a comprehensive approach versus pen tests focused, targeted approach. Hackers also bring creativity to the equation, which tends to reflect how cybercriminals continue to find new and novel means for breaching seemingly secure technologies.

Although malicious actors do use the same tools and techniques employed by pen testers, breaching technological defenses is, essentially, a criminal's job. Just as any worker brainstorms ways to do the task at hand, criminals bring never-ending creativity to their work. And while human error and simple sloppiness will always provide criminals with an open door, criminals are getting smarter and more creative. One example is the 2014 attack on Target, where criminals used the credentials of a vendor to gain access to the retailer's payment system. Another is the 2018 Ticketmaster breach, which was perpetrated via a third-party chatbot app.

The point is that this "wisdom of the crowd" works in both directions. Criminals will never go away, and they'll continue to develop new and creative methods for getting what they want. Hackers also have those same skills, but use them to find and report avenues that could potentially be exploited by criminals. With tens of thousands of white-hat hackers working to develop their own skills, learn, and even make legitimate money, the diversity of approaches and perspectives they offer is an invaluable tool for security teams.

Compared with traditional pen tests, hacker-powered security offers better results from friendly hackers using creative techniques.

Traditional Pen Testing vs. HackerOne Challenge

	TRADITIONAL PENETRATION TESTS	HACKERONE CHALLENGE
On-Demand	No	Yes
Access to Skilled Hackers / Testers	Shallow talent pool means a limited ability to match finder with scope.	The world's largest community of elite security talent, which includes world-class penetration test veterans, provide superior matching capabilities based on your program needs.
# of Researchers / Hackers per Challenge	2-4	Customizable (1, 5, 10, 500, ...)
Hacker Matching & Secure Collaboration Tools	No	Yes
Notice of Findings	Once at the end of test	In Real-Time; On-Demand
Severity of Findings	Common; Low Impact	Rare and Complex; High-Critical
Find Complex Vulnerability Chains	Rare	Common
Includes Retesting	Varies	Available
Point-in-Time or Continuous	Point-in-Time Only	Customizable (Bundles Also Available)
Dedicated Program Specialist	Yes	Yes
Managed, End-to-End Program Support	Yes	Yes
SDLC Integrations (ie, JIRA, Slack, ServiceNow, others)	No	Yes
Methodology-driven Engagements Assessments	Yes	Yes
Technical Reporting	PDF at end of testing period	Accessible In-Platform + Integrated into SDLC for easy access
Executive Summary Report	Yes	Yes (PDF)
Meet Compliance Needs (ie, PCI, HIPAA, SOC2)	Yes	Yes

More Researchers Means More Thorough Research

This crowd-based approach is also strikingly different from a pen test, which only brings a handful of researchers to any project. Typically, just 3 or so researchers conduct a pen test. Hacker-powered security programs can be private, limited, and even invitation-only based on applications or skills testing, but with over 100,000 hackers to choose from, finding dozens that fit any set of requirements is relatively easy. There is also the option to provide open access to a program, with, literally, thousands of hackers searching for vulnerabilities around the clock.

The benefit, again, is a vastly larger pool of researchers bringing an enormous diversity of skills and approaches beyond what any pen test could ever provide. The continuous aspect is also significant since weekly releases and random patches and updates are the new normal. The realities of product development, as well as the never-ending criminal effort, signal the need for a new, modern approach to pen tests.

Pay By Results For More Cost Effectiveness

Pen tests, which are provided by third-party researchers and service providers, obviously also cost money. You're paying for the expertise of the researchers, the tools required for the test, the final report, and more. A quick search shows that pen tests can be had for as low as US $1,000. More likely, however, the cost of a thorough test on a reasonable scope reaches into the US $25,000 - 50,000 range. But for a security exercise with so many potential gaps, that starts to sound like a lot of money for limited results, even when it's considered a requirement for compliance purposes.

Much of the cost of pen tests are related to the researchers' time and effort. Over just a few weeks, they devote time to preparing, testing, analyzing the results, and generating the final report. Regardless of the results, and whether they find 1 or 100 areas of concern, the cost is based on their effort and subject matter expertise.

Hacker-powered security, conversely, offers nearly unlimited effort yet the cost is directly based on actual, validated results. In time-bound challenges or continuous bug bounty programs, hackers submit reports of potential vulnerabilities. Only when those reports have been validated are hackers then paid. All the while, hackers continue providing effort in the hunt for vulnerabilities across the program's scope. So, even if thousands of hackers devote time, the cost is only based on the risks found and validated.

In the hacker-powered model, there is more bang for the buck, more flexibility to ramp resources up or down, more skills and experience to pull in, and results which are directly connected to the devoted budget.

Consider the experience of software company Open-Xchange, explained by Martin Heiland, their security officer. Heiland recounted that pen tests cost roughly US $30,000 and can be directed at specific areas of focus. On average, pen tests return about 10 "relevant findings", so US $3,000 per item. For their bug bounty program, however, they've spent far more, in excess of US $80,000, but have also identified far more vulnerabilities. The cost for bugs found via their bounty program, which they run on the HackerOne platform, averages nearly ten-times less on a per-item basis. "With our bug bounty program we see a rate of $350 per finding while getting a lot more feedback that helps us to protect our customers and learn a lot in the process," writes Heiland.

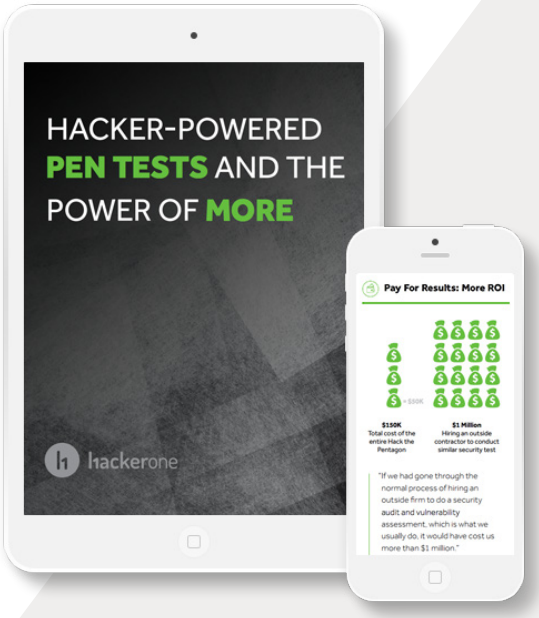
Try a Hacker-Powered Pen Test

Pen tests have been used for decades as a viable means for evaluating the security of a specific scope or technology. It's best used by organizations with advanced security practices since they tend to find many of the common risks that less mature organizations may not have yet addressed.

Regardless of security maturity, however, crowdsourced pen tests are an effective means for a continuous, creative, and broad investigation of a technology's security risks. While traditional pen tests offer a limited talent pool over a few weeks, hacker-powered pen tests bring access to tens of thousands of researchers with varying skills and broad approaches. What's more, they offer the cost benefit of paying only for validated results instead of paying for effort regardless of results.

Pen tests are a key part of any security apparatus, but the needs of rapid software development these days is far outpacing the results of periodic pen tests. The typical pen test methodologies are also falling behind the increasingly innovative methods used by criminals. The solution is to use a large and diverse set of hackers to search for and report security vulnerabilities. Crowdsourced pen tests not only augment traditional pen tests, but they also expand the benefits and add many more.

To learn how a hacker-powered pen test works, what's in the resulting report, and how security teams can work with the hackers, contact HackerOne today.

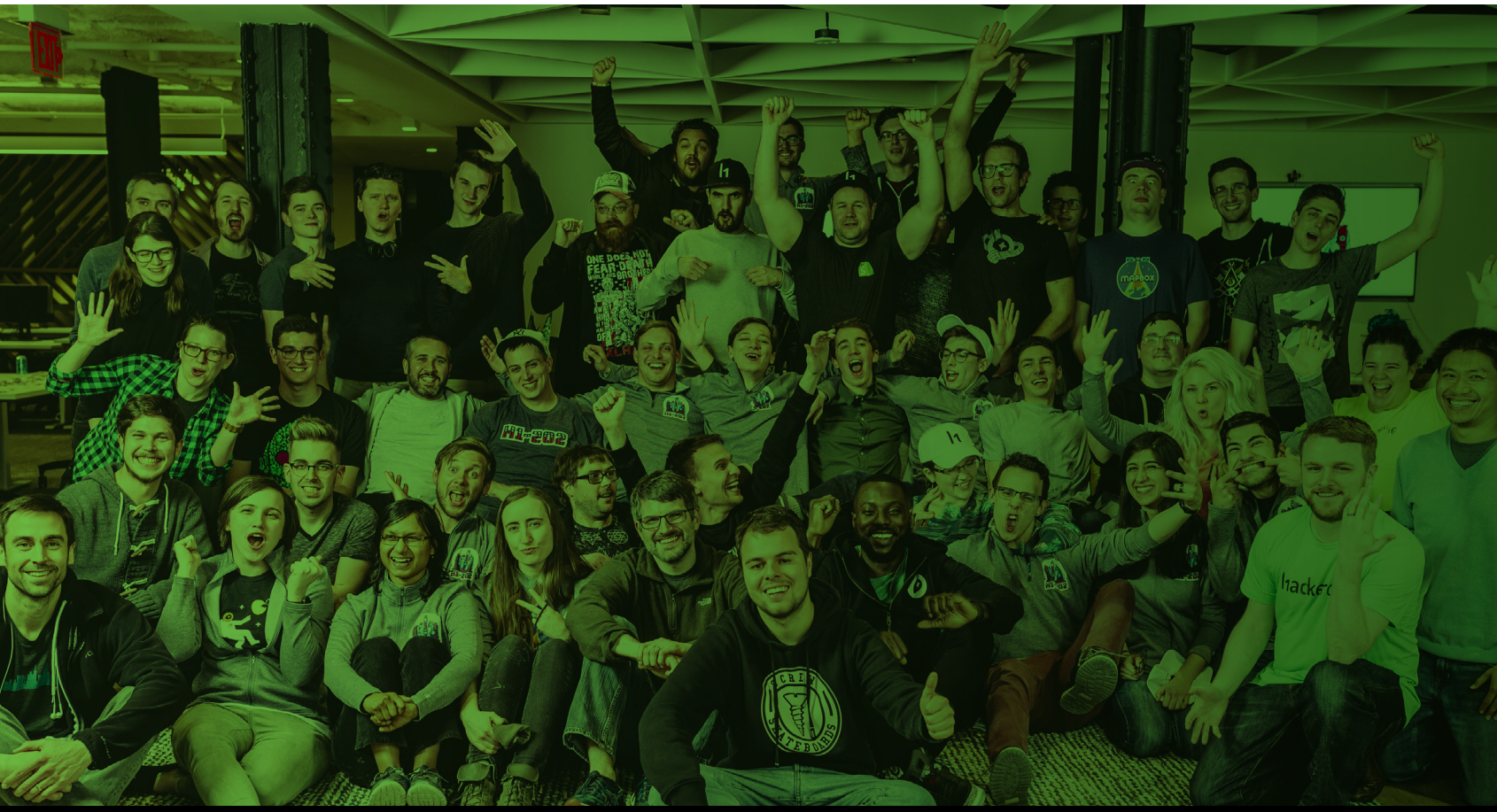


READ MORE

hackerone

ABOUT US

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,200 other organizations have partnered with HackerOne to resolve over 92,000 vulnerabilities and award over $44M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.



Contact us to get started.