Resource Guide: Types of Pentests

A penetration test (pentest) is a controlled simulated attack carried out by a third-party security expert, using the same techniques that a hacker would use. It is considered by the security community to be among **the best investments you can make** in your overall security program.

Innovative services are emerging to further refine penetration testing to meet different needs, to include Security Pursuit's Secure Network Assurance Program (SNAP)

Pentest Types	Traditional	Crowdsourced	PTaaS	Red Team	Security Pursuit SNAP
What is it?	A periodic project with a scheduled beginning and end. Attempts to look at all vulnerabilities, risk rank them, then exploit. Very controlled with a clear scope.	A vendor finds and vets large numbers of pentesters and turns them loose on your application or network. They usually do pentesting non-stop.	"Penetration Testing as a Service". As-needed pentesting. Usually coupled with ongoing vulnerability testing.	Real emulation of an attack where anything goes. It's a competitive test pitting pentester (Red Team) and your team (Blue Team).	A custom approach that leverages the control of a Traditional Pentest with more frequent testing and reporting tuned to individual client needs.
Attack Vectors	The scope and timing is pre-defined. Network (internal, external), applications, social engineering, wireless, etc..	Scope is generally defined but can be difficult to control. Timing is nonstop.	Depends on vendor, but usually applications, etc. Pentest launched by you when wanted through a dashboard.	Any attack vector works…social engineering, vuln exploits, pretext calls, physical, etc. Timing is defined but very broad…as in, "the next 2 months."	The scope and timing of each test is pre-defined according to client needs. Allows for as-needed testing as well.
Goal	Find as many vulns as possible, rank them, determine if they can be used to get into your systems. The goal is to identify exploitable vulnerabilities and threats, along with great reporting.	Test you all the time with many pentesters.	Run an automated pentest whenever you want. Great for software developers, as it can be integrated into DevOps. Good for companies that want a lot of pentesting	This is a competition for more mature security teams. The goal of the Red Team is to get in. The Goal of the Blue Team is to detect and respond.	Find as many vulns as possible, rank, and determine if they can be exploited. Frequent supplemental testing and report updates keeps reports current.
How long does it take?	Dependent on the scope, but usually 2-4 weeks.	All the time.	Anytime you want	Over a period of time, usually 1-2 months.	On-going according to a pre-determined schedule

Good	Very controlled test that goes deep on the things you care most about. Easy to budget by changing scope.	You are constantly being tested. You get a nice dashboard to see what's going on. You always have "new eyes" on your system.	You get results on a dashboard, which gives you remediation as vulns are found. Easy to fit into DevOps. Fast to schedule.	It's the best way to test your security response team with a full-on attack.	A balanced approach that aligns unique client needs for testing and reporting, giving them exactly what they want.
Bad	It's a point in time test, so it gets stale. It should be done annually at least, if not more often. Because it's a project, it's easy to postpone.	For most, it's risky! It's comparatively expensive. Access to the tester(s) is limited. Payment incentives to pentester can be misaligned. May conflict with your hosting company. Can easily hide bad pentesting skills.	Reporting is generally thru a dashboard only and canned. Depending on vendor, limited access to pentester. Very tools centric. It has a horrible name (Pentest as a Service).	Pentesters can break things. Success can be attained by one mistake, so it can end up being a very narrow test. Very skills-based, which can be hard to determine up front. Good pentesters are usually successful…just like a focused hacker.	It's slightly more expensive than traditional testing because of the expanded services.
Who's it for?	Small companies just starting on penetration testing	Companies that are big targets, can afford this, can defend themselves, and do other types of pentesting.	Software developers and larger companies that need pentesting as part of a SDLC.	Mature security teams that want to be put to the test.	Organizations who need more frequent testing and reporting.
Best Quote	"Best money you can spend if you really want to know where you're vulnerable."	"We are getting hacked constantly anyway. This way, we get reports that we can use."	"We need to test our applications before they go into production."	"Our team is so good, you're wasting your time. We're gonna see you, and we're gonna shut you down." Oh really?	"We want control over our tests, but we need to do it more frequently. Our customers, BOD, partners require current reports."
Reporting	Details on vulns and remediation. Summaries for BOD, customers, compliance, etc.	Reports are good for internal purposes. Usually a dashboard-type report.	Dashboard with findings and recommendations.	Varied depending on the event results. Can be short if pentester is successful, and can feel incomplete. Good pentesters allow for further testing.	Completely tuned to client needs and their audience. Regular updates to reports so they are never stale. Details for remediation.
What does Security Pursuit offer?	☑			☑	☑

Contact Security Pursuit to learn more about our Penetration Testing services.

sales@securitypursuit.com

720-675-ROOT (7668)