bugcrowd

DATA SHEET

PEN TEST AS A SERVICE

Network Penetration Testing

Uncover hidden vulnerabilities with specialized talent

Unnecessary firewall services, unauthorized devices, and outdated or simply misconfigured software are four significant sources of network vulnerabilities that seem relatively easy to prevent. However, the volume and velocity of infrastructure changes often make it impossible for teams to stay ahead. While regular testing can help, organizations face significant trade-offs in available options: Scanners are fast, but typically, they only surface low-hanging fruit and are almost always more noisy than useful. Traditional pen test providers leverage critical human creativity, but they do so as cumbersome consulting engagements that take too long and leave you in the dark about results.

Specialized Pen Testing for Networks

A thorough discovery of flaws in networks requires specialized knowledge, skills, and experience. For this reason, Bugcrowd Web App Pen Testing brings the talents of a global community of security researchers, precise crowd matching via our CrowdMatch™ ML technology, 24/7 visibility and the vast reservoir of vulnerability data in the Bugcrowd Security Knowledge Platform™ to bear on every pen test engagement.

Every assessment includes the following:

- Dedicated, vetted pentesters matched by skill, experience, and performance
- Strict adherence to Bugcrowd's BugHunter Methodology™ including best practices from the OWASP Testing Guide, SANS Top 25, CREST, WASC, PTES, and more
- In-depth reconnaissance, scanning, and exploitation measures for thorough network analysis
- 24/7 visibility into timelines, findings, and pentester progress through their checklist via a rich dashboard
- Validation and prioritization according to Bugcrowd's Vulnerability Rating Taxonomy (VRT)
- End-to-end program management with the industry's highest signal-to-noise ratio
- Auditor report

Key Points of Value

Buy, set up, and manage online

Cut procurement and set up time from days to hours via our easy, self-service process.

Start testing faster

Use the power of the Bugcrowd Platform to rapidly start your pen test in as little as 72 hours.

Rely on the right talent for the job

CrowdMatch™ ML technology helps align the right pentester skills and experience for the engagement.

See results in real time

Leave opaque pentesting behind. Instead, view prioritized findings as they're reported, and flow them into your SDLC for fast remediation.

Testing can be customized to suit individual testing needs--including expedited launches, re-testing, and special pentester requirements.

Network Pen Testing Methodology

Bugcrowd Network Pen Testing includes a testing methodology that blends key organizational and operational best practices of leading industry standards to drive both risk reduction and compliance for customers with varying priorities. Testing is executed through four critical phases: Reconnaissance, Enumeration, Documentation, and Exploitation. Each phase is executed in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risk. A blend of organizational and operational best practices provides both coverage, and meaningful results.

Reconnaissance and Enumeration

Utilize various search engines and data sources to uncover assets and information helpful for understanding attack vectors. This may include, but is not limited to the following:

- External asset discovery using search engines, public code repositories and paid services
- Credentials or keys leaked on GitHub, Pastebin, and others
- Usernames, emails, passwords and other information leaked as part of past breaches
- Internal assets, known software, and others
- Check for the ability to perform a zone transfer on in-scope DNS servers
- Enumerate company acquisitions through public records and news sources

Scanning

Combine automation, tooling, and human ingenuity

- Fully scan the range of in-scope targets on all TCP and UDP ports
- Enumerate and document all in-scope services and version numbers
- Check for unencrypted services (Telnet, http, and others)
- Check for misconfigured services or DNS records allowing for subdomain takeovers
- Review services to determine if any are exposing sensitive information
- Analyze returned error codes and stack traces for additional information
- Optional automated scans to detect “low-hanging fruit”

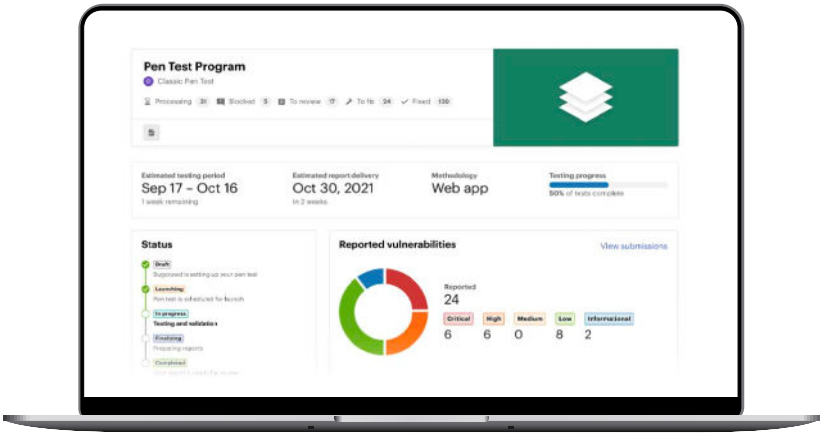
Exploitation and Documentation

Verify security weaknesses and collect results

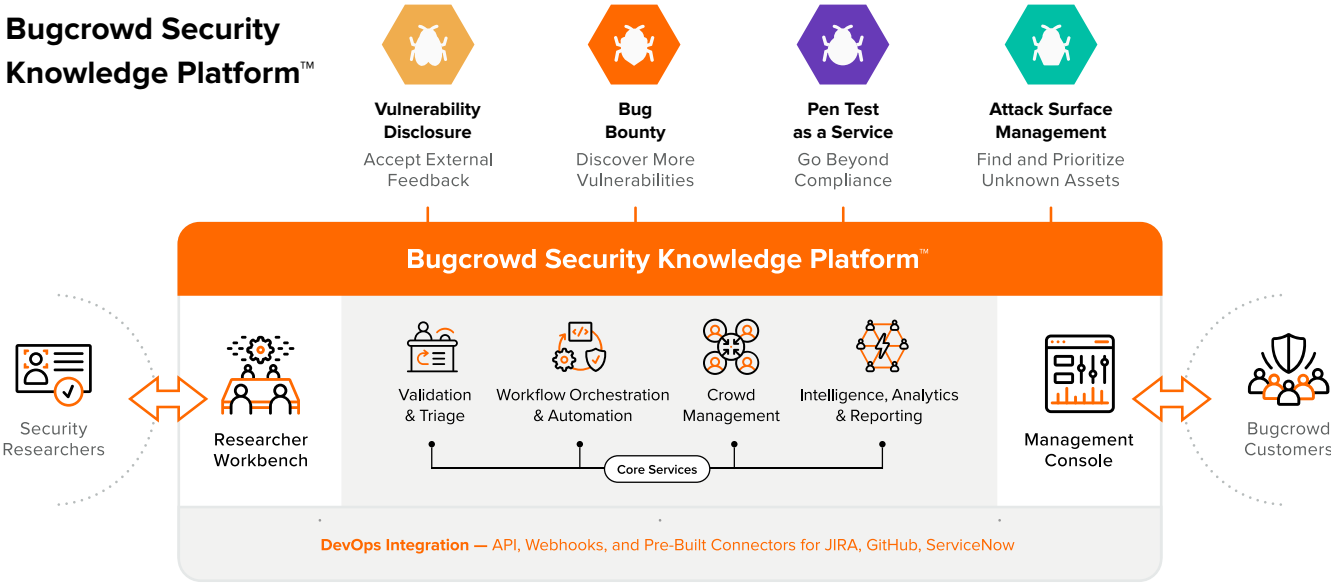
- Test for authorization bypasses (insecure implementations of OAuth, SAML, and others)
- Leverage discovered services to obtain additional information about the targets
- Check for service misconfigurations and deployment mistakes
- Attempt to discover exposed files containing sensitive information (database backups, open git repositories, and others)
- Check for default/weak credentials on all available services (HTTP, telnet SSH, SNMP, and others)
- Check for weak encryption (SSL/TLS ciphers, older protocols, and others)
- Check for known/public exploits on discovered services by cross-referencing software version numbers against public vulnerability databases
- Check for presence of sensitive information that is publicly available on any service (e.g. documents available via anonymous FTP)
- Attempt calculated brute-forcing on available services based on information gathered earlier in the assessment
- Test any available web servers for server-side vulnerabilities, including but not limited to the following:
  - Authentication bypasses
  - SQL Injection (SQLi)
  - Remote Code Execution (RCE)
  - XML Entity Injection (XXE)
  - Server-side request forgery (SSRF)
  - File inclusion (LFI/RFI/AFI)

How It Works

The Bugcrowd Security Knowledge Platform™ makes it easy to configure and launch pen tests for any asset. After building a pentester team per your exact needs, we'll launch your pen test within days and give you 24/7 access to prioritized results, along with test status and progress, in a rich dashboard. When your test is complete, you can download a detailed report for compliance directly inside your dashboard.



Bugcrowd Security Knowledge Platform™



Right Crowd, Right Time

Need special skills? We match the right trusted hackers to your needs and environment across hundreds of dimensions using AI (CrowdMatch™).

Engineered Triage at Scale

Using an advanced toolbox in our the platform, our global team rapidly validates and triages submissions, with P1s often handled within hours.

Insights From Security Knowledge Graph

We apply knowledge developed over a decade of experience across thousands of customer programs to help you make continuous improvements.

Works With Your Existing Processes

The platform integrates with your existing tools and processes to ensure that applications and APIs are continuously tested before they ship.