bugcrowd

DATA SHEET

PENETRATION TESTING

Network Penetration Testing

Bugcrowd Penetration Testing-as-a-Service Solution

Summary

Unnecessary firewall services, unauthorized devices, and outdated or simply misconfigured software are four significant sources of network vulnerabilities that seem relatively easy to prevent.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. For example, companies can implement scanners quickly, but they typically only surface low-hanging fruit and are almost always more noisy than helpful. Traditional pen test providers leverage necessary human creativity, but they come with limited capacity or at the cost of significant scheduling delays.

Specialized Pen Testing for Web Apps

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, rapid validation and triage, and the vast reservoir of vulnerability knowledge residing 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
- 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
- QSAC-Assessed compliance report

Key Points of Value

Start testing faster

Use the power of the Bugcrowd Platform and the Crowd to rapidly start your testing in as little as 72 hours.

Expert testers are matched to your requirements

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

Get real-time results

Vulnerabilities are triaged, validated, and then made available in real time via the Bugcrowd Platform and in your integrated tools of choice to enable rapid remediation.

Packages can be modified and expanded to suit individual testing needs; indeed, they may include expedited report delivery, executive reporting, vulnerability re-testing, and even options to incentivize greater vulnerability discovery.

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

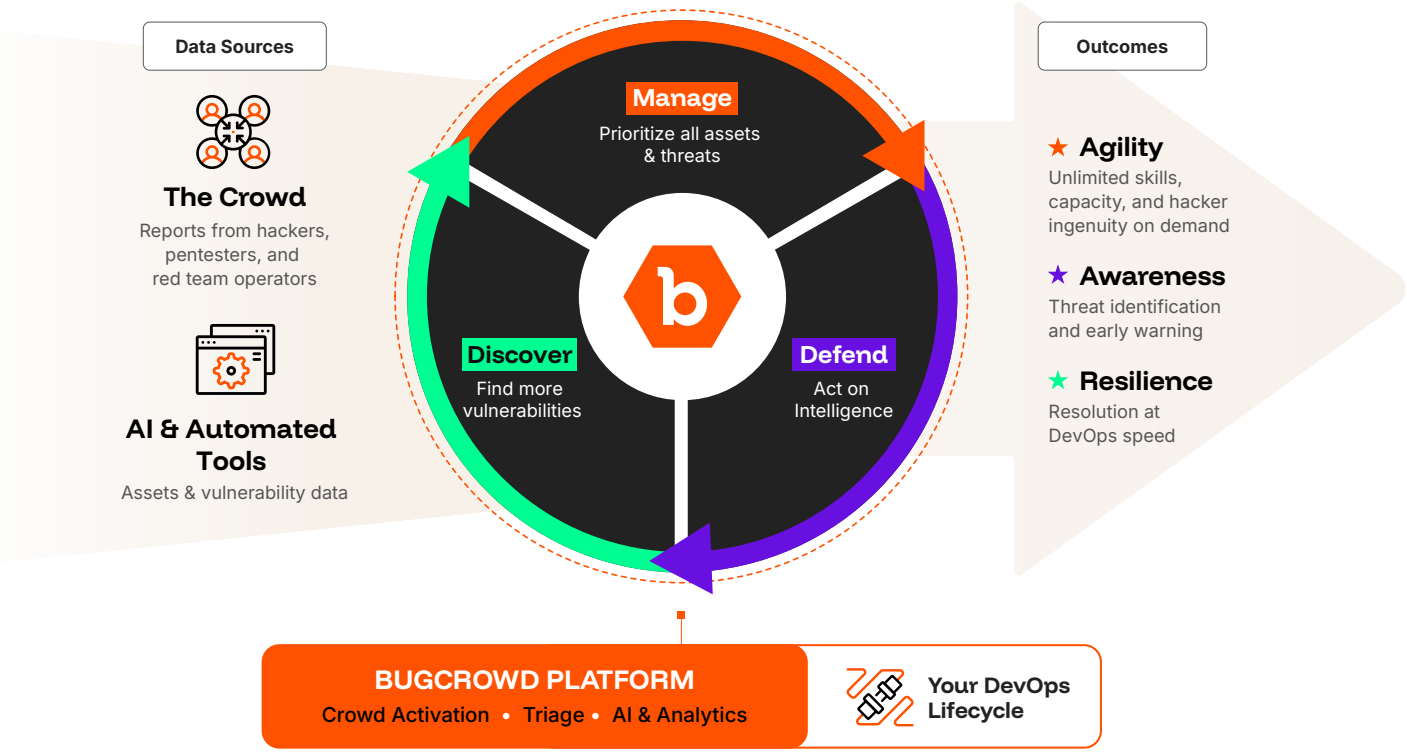
- Fully scan the range of in-scope targets on all TCP and UDP ports
- Enumerate and document all in-scope services and version numbers
- Check for unencrypted services (Telnet, http, and others)
- Check for misconfigured services or DNS records allowing for subdomain takeovers
- Review services to determine 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)

Bugcrowd Platform



The Bugcrowd Platform fuses AI with real-time, crowdsourced intelligence from the world's top ethical hackers, pentesters, and red teamers (aka The Crowd), as well as from automated tools that generate asset, threat, and vulnerability data. The powerful combination of human creativity and automation empowers you to continuously:

Agility

Augment Your Team On Demand

- Attacker mindset on tap for vulnerability discovery, pen testing, and red teaming
- 350+ skill sets and certifications available
- Crowd curation and activation guided by data and AI

Awareness

See and Prioritize Emerging Threats

- Continuous vulnerability intake, validation, and triage at scale
- 24/7 triage coverage with same-day response for P1s
- Early warning of emerging vulnerabilities

Resilience

Continuously Improve Security Posture

- Actionable reporting, benchmarking, and recommendations
- Directly integrates with existing tools for change at DevOps speed
- Deep bench of solution & support specialists at your side for quick wins and long-term ROI

mastercard indeed credit karma Pinterest NASA ATLASSIAN