BLACKDUCK®

GUIDE

Penetration Testing: A Buyer's Guide

Not all pen testing is created equal

Data breaches continue to plague organizations—whether they're targeted attacks from outside or malicious insiders. According to the 2020 IBM "Cost of Data Breach" report, 52% of breaches were caused by a malicious attack and the average total cost of a breach was $3.86 million. Many of these breaches are the result of combinations of errors or vulnerabilities, with attackers working their way through a system and exploiting any and all weaknesses they find.

This is a clarion call for organizations to secure their applications and network before a breach compromises valuable data and tarnishes their brand reputation. Development and application security (AppSec) teams use a variety of testing techniques to secure their networks and applications, including static application security testing (SAST) and software composition analysis (SCA) solutions.

But many vulnerabilities can be detected only during runtime tests and release phases. While SAST and SCA tools identify security vulnerabilities down to line of code, they cannot identify runtime or environment risks. As a result, developers don't get a complete picture of multivector attack vulnerabilities in their system. That's why many organizations use dynamic application security testing (DAST) and penetration testing during QA, late stages of production, or in some cases, after deployment, to detect vulnerabilities that cannot be found earlier in the development cycle.

Phases of pen testing

- **Reconnaissance.** Gather as much information as possible from public and private sources to map out the target's attack surface and possible vulnerabilities.
- **Scanning.** Examine the target website or system for weaknesses, including open services, application security issues, and open source vulnerabilities.
- **Gain access.** Choose the best tools and techniques to gain access to the system, whether through a weakness, such as SQL injection, or through malware, social engineering, or something else.
- **Maintain access.** Stay connected long enough to demonstrate the potential impact of a breach, such as exfiltrating or modifying data, or abusing functionality.

Penetration testing

There are myriad ways to break into web applications and networks, and hacking techniques are always evolving. It's just not possible for smaller development and security teams to keep up with the ever-changing security testing landscape or get a holistic view of the health of their applications and networks. Security teams can use external penetration testing to round out their testing throughout the software development life cycle (SDLC), overcome resource constraints internally, and meet compliance requirements.

Pen testing is a foundational layer for enterprise security. It's an authorized simulated attack on a system that looks at a system the way a hacker does, using the same techniques and tools attackers use to identify weaknesses in a system and applications at runtime. Paired with other methods, such SAST, SCA, threat modeling, and architecture risk analysis, pen testing helps provide a holistic view of applications and the network.

Using a combination of automatic scanning and manual testing in a simulated real-world environment, penetration testing can identify and prioritize weaknesses from a combination of vulnerabilities to detect the highest risks. This enables developers to find and fix the weaknesses before they can be exploited.

Key benefits of pen testing solutions

Comprehensive vulnerability and security risk reporting

Pen testing enables developers to find and fix runtime vulnerabilities in the final development stages or after deployment. Run in a simulated environment to eliminate business interruptions, pen testing reduces overall security risk by finding weaknesses in the system and determining the strength of existing controls.

Actionable findings for development teams

Pen testing identifies weaknesses in applications and network services, including complex, multivector vulnerabilities, to determine if intrusion is possible. These findings empower developers to find and fix issues before they can be exploited by bad actors.

Low false-positive rates

Using a combination of automated and manual procedures, pen testers manually verify results and ensure a high degree of accuracy. This enables organizations to focus security resources on the high-priority vulnerabilities that require additional attention to identify, verify, and resolve.

Seamless integration into development and testing environments

Pen testing solutions seamlessly fit at the end of the continuous integration / continuous delivery (CI/CD) pipeline and provide insight into the runtime environment. They work in tandem with SAST and IAST, which identify source code errors, to create more-secure software and systems.

At a glance

Benefits of pen testing

- Comprehensive assessments in the runtime environment
- Identification of complex, multivector vulnerabilities
- Accurate results enable triage and low false-positive rates
- Seamless integration into the current SDLC and CI/CD pipeline
- Real-world simulation of attacks to prioritize vulnerabilities based on exploitation risk
- Compliance with industry regulations and legal requirements
- Remediation guidance vetted in the real world with similar applications

What to look for in a pen testing provider

There are several factors to consider when selection a penetration testing solution—and many vendors to choose from. No matter which solution your organization chooses, these are the minimum requirements to look for.

Experience

Ensure the team has a documented process and real-world experience across testing tools and techniques, and the platforms, application types, and programming languages used in your organization.

Security

The penetration testing solution should ensure that your data remains secure. This includes providing clear information on security process, how it logs and maintains records of who is accessing the data, and how it handles your data and disposes of it after completing the job. And the vendor should share testing results only with authorized personnel.

Compliance support

Look for a solution that fully supports compliance with data privacy and security regulations, including PCI DSS, HIPAA, NIST, GDPR, OWASP Top 10, SANS/CEW, or other sets of compliance standards relevant for your business and industry.

Manual and automated testing styles

The best penetration testing solutions use automated tools that focus on exploratory risk analysis including integrity checks and business logic data validation. They also include manual testing techniques to explore attacks beyond a standard list. Manual testing additionally helps eliminate false positives and provides more detail to explain findings.

Flexible testing model

There is no one-size-fits-all solution for pen testing. Work with a testing provider that uses tools to support different testing types, such as:

- Tools that discover network hosts and open ports
- Vulnerability scanners for network services, web applications, and APIs
- Proxy tools
- Exploitation tools to achieve system footholds or access to assets
- Post-exploitation tools for interacting with systems, maintaining and expanding access, and achieving attack objectives

Detailed security guidance and remediation advice

Pen testing solutions should provide developers and security teams with a detailed, customized report that offers contextual information about vulnerabilities identified during the assessment, and recommendations for actionable mitigation and remediation strategies.

Support for modern technologies

More organizations are using APIs, microservices, and serverless architecture. Penetration testing solutions should help identify vulnerabilities in back-end logic and detect and trace data flows and any tainted data used.

Comprehensive rules of engagement

The most effective penetration testing services use rules of engagement to set expectations for the process and avoid misunderstandings. Rules include elements such as test parameters, targets, and escalation procedures.

Questions to ask a potential penetration testing solution provider

- Are there any restrictions on the number of applications the vendor can pen test?
- What reputation does the vendor have in the AppSec space?
- Does the pen testing vendor have experience in, and understand the needs of, your industry?
- What expertise or resources can the vendor provide to support developers and for general tech support?
- What programming languages, platforms, and frameworks does the pen testing tool support?
- What regulations and compliance standards does the pen testing solution support?
- Does the pen testing tool inspect multiple points of entry into the organization?
- Does the pen testing tool deal with social engineering, such as employee awareness, physical safeguards, or data disposal?
- What steps will be taken if the pen testing detects an active compromise to the system?
- Does the pen testing vendor provide clear reporting of vulnerabilities, with actionable remediation steps?
- Does the vendor have well-rounded experience in a broad variety of pen testing, including for web apps, networks, APIs, thick clients, embedded devices, and more?

Black Duck penetration testing

Black Duck penetration testing thoroughly and systematically finds and eliminates business-critical vulnerabilities in running web applications and web services, including networks, APIs, thick clients, and embedded devices—without access to source code. You choose from several depths of managed pen testing, tuning the level of testing based on the risk profile of each tested application. With over two decades of experience providing testing services, Black Duck has developed a refined, precise run book for penetration testing. With Black Duck experts doing the testing, your in-house security team can focus on more strategic security objectives. Black Duck penetration testing is:

- **Flexible.** Manage assessments, scheduling, depth of testing.
- **Consistent.** The same high-quality pen testing results for any application.
- **Comprehensive.** A blended manual and tool-based approach includes thorough analysis of results, detailed reporting, and actionable remediation guidance.
- **Actionable.** Developers get specific remediation guidance.

Regardless of your organization's application test and security maturity, Black Duck penetration testing can provide numerous benefits:

- It's ideal for protecting against complex, multivector attacks.
- It helps find runtime vulnerabilities and determines if intrusion is possible, reducing the risk of a breach.
- We walk you through your test results and help you develop a remediation plan best suited to your needs.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.