PENETRATION TESTING EXPLAINED

Penetration testing provides a real-world test of your security posture by sending an ethical hacker to break in using the same techniques as actual bad guys. While most people picture pen testing as someone cracking lines of code, the process entails far more than that.
Here's an overview of a pen test from initial scoping to final validation:

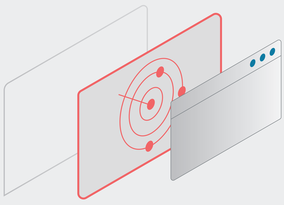
1 SCOPING

In this phase, clients and testers agree on the ground rules, such as whether the test of a web app extends to the infrastructure behind it. The team also decides whether to alert the client's IT team about the test or to let them practice stopping what they think is an actual attack.

2 RECON

INTEL GATHERING

Like real hackers, good pen testers use the web, social media and other public sources to identify individuals and parts of the organization to target. They also uncover technical details through port scanning, network sniffing and more.

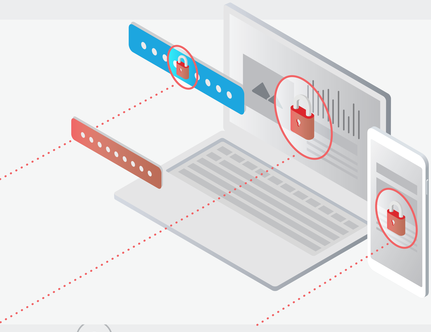


VULNERABILITY SCANNING

Automated tools scan your system for known vulnerabilities such as open ports and unpatched software that the human pen tester can use in their attack.

SOCIAL ENGINEERING

It's easier to hack a person than a server. So pen testers often try to fool someone into giving up their system credentials through phishing, pretexting phone calls, etc.



3 HACKING INTO THE SYSTEM

Armed with research, ethical hackers attack the system using known vulnerabilities; predictable or leaked passwords; spoofed login sites or devices; and more. Once they gain a foothold, pen testers pivot through the environment to see how much data they can access.

4 ORGANIZING FINDINGS

The pen tester begins listing risks they discover and categorizing them according to a common standard such as the OWASP Top 10 for web apps. Risk categories include broken access control, cryptographic failure, insecure design and more.

5 REPORTING

Now the pen tester formats their work into an understandable, actionable report for the client team. A good reporting process includes an executive summary, an in-depth technical report and an action plan listing recommended remediations.

6 REMEDIATING

Armed with the detailed report, the client's team can begin remediating moderate and high risks.

7 VALIDATING

After the IT team remediates risks highlighted in the external portion of the pen test, the pen tester returns to confirm that each risk has been eliminated. This confirmation is included as part of all external engagements.

Penetration Testing Services

Click here to learn more about penetration testing services from HBS.

HBS