HBS

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 identify the environments, systems, applications, etc., that are within scope for the pen testing engagement. The team will also provide recommendations for which elements should or should not be in scope based on risk and potential business impact.

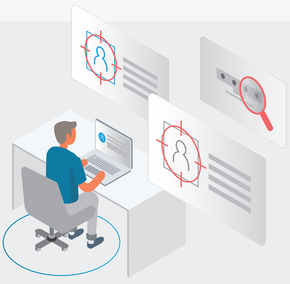
2 KICKOFF

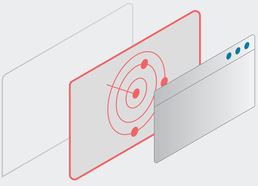
In the kickoff call, the team confirms the scope of testing, sets the ground rules for when testing will be performed, and determines how communications will be handled.

3 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.



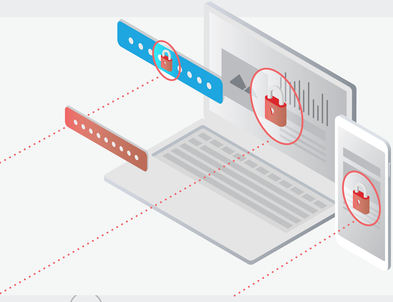


VULNERABILITY SCANNING

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, in some cases, pen testers might try to fool someone into giving up their system credentials through phishing, vishing, etc.



4 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.

5 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.

6 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.

7 REMEDIATING

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

8 VALIDATING

After the IT team remediates risks identified during the testing, retesting by the pen tester should take place to determine the effectiveness of remediation.

Penetration Testing Services

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

HBS