TYPES OF PENETRATION TESTING

A thorough penetration testing campaign involves social engineering, vulnerability scanning, and the manual hacking of computer systems, networks, and web applications. This overview shows how a professional pen testing team tries to exploit a variety of attack vectors, just as a real hacker would.

SOCIAL ENGINEERING: HACKING HUMANS

1 PHISHING

Testers craft emails that seem to be from a trusted source and invite recipients to either supply their login credentials or click on a malicious link or attachment.

2 PRETEXTING

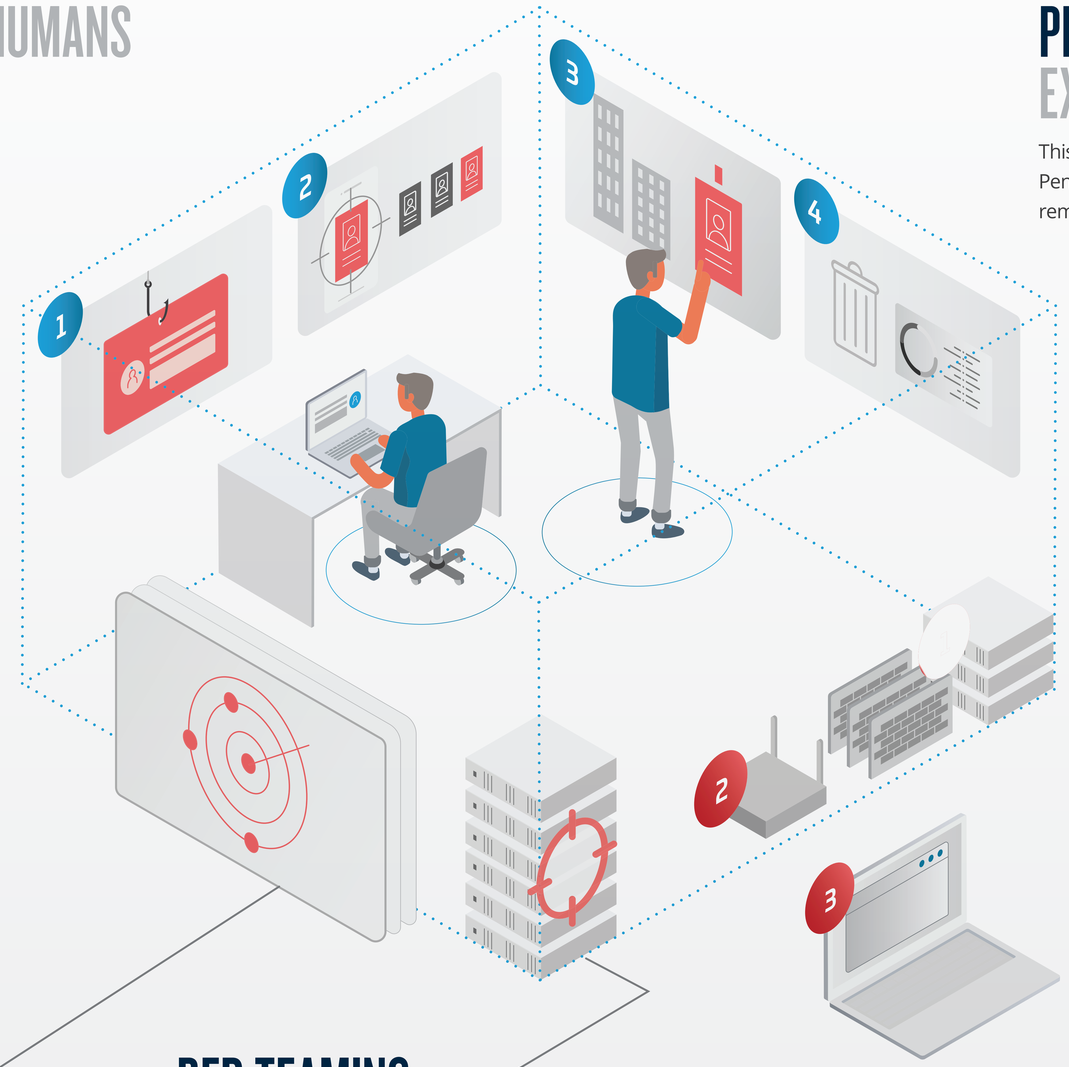
Testers call targeted people and ask for sensitive information such as login credentials or fool the user into performing a malicious action. Callers frequently impersonate a Call Center rep or a fellow employee from another division.

3 FACILITY ACCESS

Old-fashioned physical intrusion still plays a role. Testers may slide through an open door in a group of employees. Or they may look for vulnerable entrances such as loading docks, maintenance entrances or designated smoking areas. Testers sometimes pose as maintenance workers and talk their way into sensitive parts of the facility.

4 DUMPSTER DIVING

Just like real hackers, testers know they often can find sensitive information in the trash. This might include credit card receipts, travel information, network diagrams, device inventories with IP addresses, contact lists, and more.



VULNERABILITY SCANNING: DISCOVERING WEAKNESSES

Automated tools seek known security vulnerabilities in your systems such as unpatched software or open ports. The scans reveal risks that may directly impact your organization and point pen testers to areas they can try to exploit.

RED TEAMING: EMULATING ADVANCED THREATS

Here, pen testers take a more adversarial approach as they go after specific targets. This type of advanced, focused test emulates Tactics, Techniques and Procedures (TTPs) of mature threat actors. The Red Team attempts to remain invisible to the systems' defenders (known as the Blue Team).

PENETRATION TESTING: MANUALLY EXPLOITING VULNERABLITIES

This proactive approach adds human expertise to the testing process. Penetration testers attempt to exploit vulnerabilities and recommend remediations before hackers can exploit the gaps.

1 NETWORK & INFRASTRUCTURE

Infrastructure penetration testing identifies security weaknesses within your network. Testers look for flaws such as outdated software, missing patches, improper security configurations, weak communication algorithms, command injection, etc. Infrastructure penetration tests often include testing of firewalls, switches, virtual and physical servers, and workstations.

2 WIRELESS PENETRATION TESTING

Hackers can leverage wireless capabilities to infiltrate an organization's secured environment, even if some access and physical security controls are in place. Pen testers map access points in the wireless landscape and gain access to the wireless network. Then they attempt to exploit weaknesses in the network to gain access to privileged areas and demonstrate the potential impact of a wireless network breach.

3 WEB APPLICATIONS

Web applications often process and/or store sensitive information including credit card data, personally identifiable information (PII), and proprietary data. And web apps are frequently vulnerable due to their complexity and rapid development cycles. That's why about 40% of all breaches involve web apps. And that's why a well-rounded pen test includes any web apps the company uses.

Penetration Testing Services

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

HBS