TYPES OF **PENETRATION TESTING**

A thorough penetration testing campaign involves **social engineering, vulnerability exploitation, 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.

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

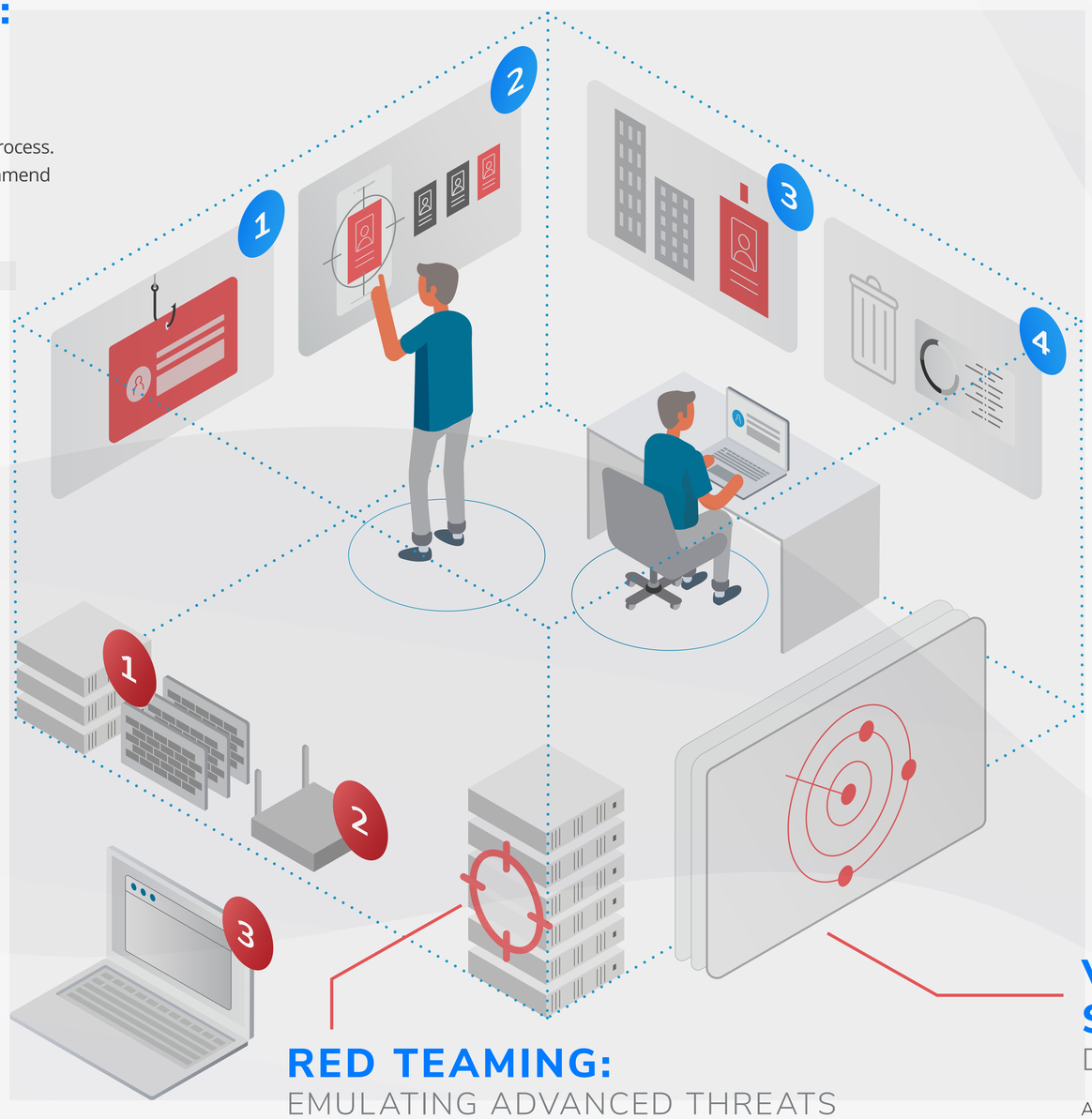
Infrastructure penetration testing identifies and exploits weaknesses and vulnerabilities within your network and connected systems. Testers evaluate firewalls, switches, physical and virtual machines, workstations—and take a closer look at Active Directory and web-based authentication, two of the most common entry points for attackers.

2 WIRELESS PEN 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 30% of all breaches involve web apps. And that's why a well-rounded pen test includes any web apps the company uses.



SOCIAL ENGINEERING:
HACKING HUMANS

1 PHISHING

Testers craft emails that appear to come from a trusted source—like IT, HR, or a known vendor—and try to trick recipients into clicking a malicious link, opening an attachment, or entering login credentials.

2 VISHING

Testers call targeted people, posing as IT support, HR, or a colleague from another department with the goal of tricking the user into sharing credentials or taking a risky action—like visiting a malicious site or changing security settings.

3 FACILITY ACCESS

Old-fashioned physical intrusion still plays a role. Testers may tailgate 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 MEDIA DROPS

Testers mimic real attackers by planting USB drives that appear to contain information that might entice an employee to plug in the drive and open the files. A single plugged-in drive can act like an attacker at the keyboard, opening the door from the inside.

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).

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 before an actual attacker does.

Penetration Testing Services

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

HBS