Penetration testing

An effective security plan relies on regular testing to find an organization's weaknesses. Previously, you learned that **vulnerability assessments**, the internal review process of an organization's security systems, are used to design defense strategies based on system weaknesses. In this reading, you'll learn how security teams evaluate the effectiveness of their defenses using penetration testing.

Penetration testing

A **penetration test**, or pen test, is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. The simulated attack in a pen test involves using the same tools and techniques as malicious actors in order to mimic a real life attack. Since a pen test is an authorized attack, it is considered to be a form of ethical hacking. Unlike a vulnerability assessment that finds weaknesses in a system's security, a pen test exploits those weaknesses to determine the potential consequences if the system breaks or gets broken into by a threat actor.

For example, the cybersecurity team at a financial company might simulate an attack on their banking app to determine if there are weaknesses that would allow an attacker to steal customer information or illegally transfer funds. If the pen test uncovers misconfigurations, the team can address them and improve the overall security of the app.

Note: Organizations that are regulated by PCI DSS, HIPAA, or GDPR must routinely perform penetration testing to maintain compliance standards.

Learning from varied perspectives

These authorized attacks are performed by pen testers who are skilled in programming and network architecture. Depending on their objectives, organizations might use a few different approaches to penetration testing:

- Red team tests *simulate attacks* to identify vulnerabilities in systems, networks, or applications.
- Blue team tests focus on *defense and incident response* to validate an organization's existing security systems.
- Purple team tests are *collaborative*, focusing on improving the security posture of the organization by combining elements of red and blue team exercises.

Red team tests are commonly performed by independent pen testers who are hired to evaluate internal systems. Although, cybersecurity teams may also have their own pen testing experts. Regardless of the approach, penetration testers must make an important decision before simulating an attack: *How much access and information do I need?*

Penetration testing strategies

There are three common penetration testing strategies:

- **Open-box testing** is when the tester has the same privileged access that an internal developer would have—information like system architecture, data flow, and network

diagrams. This strategy goes by several different names, including internal, full knowledge, white-box, and clear-box penetration testing.
- **Closed-box testing** is when the tester has little to no access to internal systems—similar to a malicious hacker. This strategy is sometimes referred to as external, black-box, or zero knowledge penetration testing.
- **Partial knowledge testing** is when the tester has limited access and knowledge of an internal system—for example, a customer service representative. This strategy is also known as gray-box testing.

Closed box testers tend to produce the most accurate simulations of a real-world attack. Nevertheless, each strategy produces valuable results by demonstrating how an attacker might infiltrate a system and what information they could access.

Becoming a penetration tester

Penetration testers are in-demand in the fast growing field of cybersecurity. All of the skills you're learning in this program can help you advance towards a career in pen testing:

- Network and application security
- Experience with operating systems, like Linux
- Vulnerability analysis and threat modeling
- Detection and response tools
- Programming languages, like Python and BASH
- Communication skills

Programming skills are very helpful in penetration testing because it's often performed on software and IT systems. With enough practice and dedication, cybersecurity professionals at any level can develop the skills needed to be a pen tester.

Bug bounty programs

Organizations commonly run bug bounty programs which offer freelance pen testers financial rewards for finding and reporting vulnerabilities in their products. Bug bounties are great opportunities for amateur security professionals to participate and grow their skills.

Pro tip: HackerOne is a community of ethical hackers where you can find active bug bounties to participate in.

Key takeaways

A major risk for organizations is malicious hackers breaking into their systems. Penetration testing is another way for organizations to secure their systems. Security teams use these simulated attacks to get a clearer picture of weaknesses in their defenses. There's a growing need for specialized security professionals in this field. Even if you start out assisting with these activities, there's plenty of opportunities to grow and learn the skills to be a pen tester.