Penetration Testing: Assessment Types

Today, We're diving into the different types of assessments used in penetration testing. Understanding these categories will help you determine the right approach for a specific situation.

There are three main types outlined in the objectives:

1. Goals-Based or Objectives-Based Assessments:

Imagine a company just developed a new security system. They want to know if it's actually secure before relying on it. This is a goals-based assessment. The tester is focusing on a specific objective: validating the new security design.

Here are some other real-world examples:

- A company is about to launch a new mobile app. They want to test the app's security before releasing it to the public. This ensures the app doesn't have vulnerabilities attackers can exploit.
- A company just acquired another company. They want to assess the security posture of the acquired company's systems. This helps identify any potential security risks before they become a problem.

2. Compliance-Based Assessments:

Many laws and regulations have specific security requirements. Compliance-based assessments ensure an organization meets those requirements.

For instance, a company might need to comply with PCI DSS (Payment Card Industry Data Security Standard) if they handle credit card information. A penetration test can help verify they meet the security standards outlined in PCI DSS.

Here's another example:

- A healthcare provider needs to comply with HIPAA (Health Insurance Portability and Accountability Act) regulations. A penetration test can ensure they have adequate security measures in place to protect patient data.

3. Red Team Assessments:

Imagine a military exercise where a "red team" simulates an enemy attack. Red team assessments are similar. Testers act like malicious attackers, trying to gain access to sensitive data or systems.

Unlike other assessments, red teams aren't focused on finding every single flaw. Their goal is to see if they can achieve their objective (e.g., stealing data) just like a real attacker would.

Here's why red team assessments are valuable:

- They test how well your security team responds to an actual attack.
- They help identify weaknesses in your security procedures and designs.

Remember, red team assessments are more intense than typical penetration tests. They require careful planning and coordination to avoid causing disruptions.

Key takeaway: The type of assessment you choose depends on your specific goals. Goals-based assessments are good for validating security designs or testing new systems. Compliance-based assessments ensure you meet regulatory requirements. Red team assessments test your security posture against real-world attack scenarios.

By understanding these different types of assessments, you'll be well-equipped to choose the right approach for your penetration testing needs.