Understanding Penetration Testing: Beyond Vulnerability Scans

Automated "Penetration Tests" (Vulnerability Scans)

A standard vulnerability scan is a good hygiene assessment to determine where a company should look to harden their environment. While useful, it does not mimic true hacker tradecraft, include lateral movement, establish external command and control, or trigger real-time threat response.

- **SCOPE:** Primarily automated; focuses on identifying vulnerabilities
- **METHOD:** Uses software tools to scan for known vulnerabilities

True Penetration Testing

Penetration tests are simulated cyberattacks on your systems conducted by ethical hackers (known as pen testers) with an organization's permission. It is a manual, in-depth process, tailored to your unique environment, aiming to uncover weaknesses and demonstrate their impact. This is done by using tools and techniques that malicious actors might use in an attack, tailored for your unique environment. They probe, then exploit, gaps in defenses that will likely trigger a real-time threat response.

- **SCOPE:** Comprehensive; simulates real-world attacks by mimicking threat actor behaviors
- **METHOD:** Involves hands-on keyboard activities, realistic tradecraft, and lateral movement

Key Considerations When Choosing a Test

- **TARGET SPECIFICS:** If testing a particular application or environment for weaknesses, a true penetration test can provide in-depth analysis. An automated one will have less depth, visibility, and realism as it does not pivot through the environment.
- **BROAD ANALYSIS:** For a general assessment of potential vulnerabilities across the environment, vulnerability scanning tools can identify areas of improvement but may not always confirm exploitability.
- **CONFIGURATION AND PERMISSIONS:** To assess the impact of network misconfigurations and permission levels, security audits can be effective.
- **SECURITY SOLUTION TESTING:** To evaluate the ability of security solutions to detect and prevent attacks, specific testing of defense evasion techniques used by adversaries should be considered.
- **FULL-SCALE ATTACK SIMULATION:** A comprehensive red team operation or hands-on penetration test is crucial to understand the full lifecycle of an attack and the effectiveness of the security posture at each stage. Skipping one of the most important steps, such as gaining initial access, is a major gap in some vulnerability scans that make the simulated attack chain much less realistic.

Blackpoint Cyber is focused on the endpoint level, with an emphasis on detecting the presence of:

Tradecraft | Lateral movement | Legitimate IT tool exploitation

Combining network visualization, security data analysis, and endpoint security, Blackpoint's Active Cybersecurity suite rapidly detects and neutralizes lateral movement and adversarial tradecraft in its earliest stages to safeguard our partners 24/7.

Partner with Blackpoint's Active-SOC services that will win the cyber fight for you.

blackpointcyber.com