Understanding Penetration Testing: Beyond Vulnerability Scans

Automated Penetration Tests (Vulnerability Scans)

A standard penetration test is a good assessment to determine where a company should look to harden their environment. However, they're typically automated scans that showcase vulnerabilities at the network level, which do not account for tradecraft and lateral spread. Additionally, these automated scans will often not trigger a real-time response from your security product(s).

- **SCOPE:** Primarily automated; focuses on identifying network-level vulnerabilities.
- **METHOD:** Uses software tools to scan for known vulnerabilities in the network infrastructure.
- **LIMITATIONS:** Does not involve tradecraft, lateral movement, or real-time threat response.
  - May not detect hidden shares, insider threats, or sophisticated attack vectors.
  - May not trigger the response of your security product since it isn't a hands-on, real-time attack.

True Penetration Testing with Blackpoint Cyber

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

- Tradecraft
- Lateral movement
- Legitimate IT tool exploitation
- Privileged remote executions

Combining network visualization, insider threat monitoring, traffic 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.

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

Key Considerations When Choosing a Test

- **TARGET SPECIFICS:** If testing a particular application or system for vulnerabilities (including zero-days), a true penetration test can provide in-depth analysis.
- **BROAD ANALYSIS:** For a general assessment of potential vulnerabilities across the environment, vulnerability scanning tools can identify areas for improvement but may not always confirm exploitability.
- **CONFIGURATION AND PERMISSIONS:** To assess the impact of network misconfigurations and permission levels, security audits using tools like Sharphound and Bloodhound 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 penetration tests that makes the simulated attack chain much less realistic.

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

blackpointcyber.com