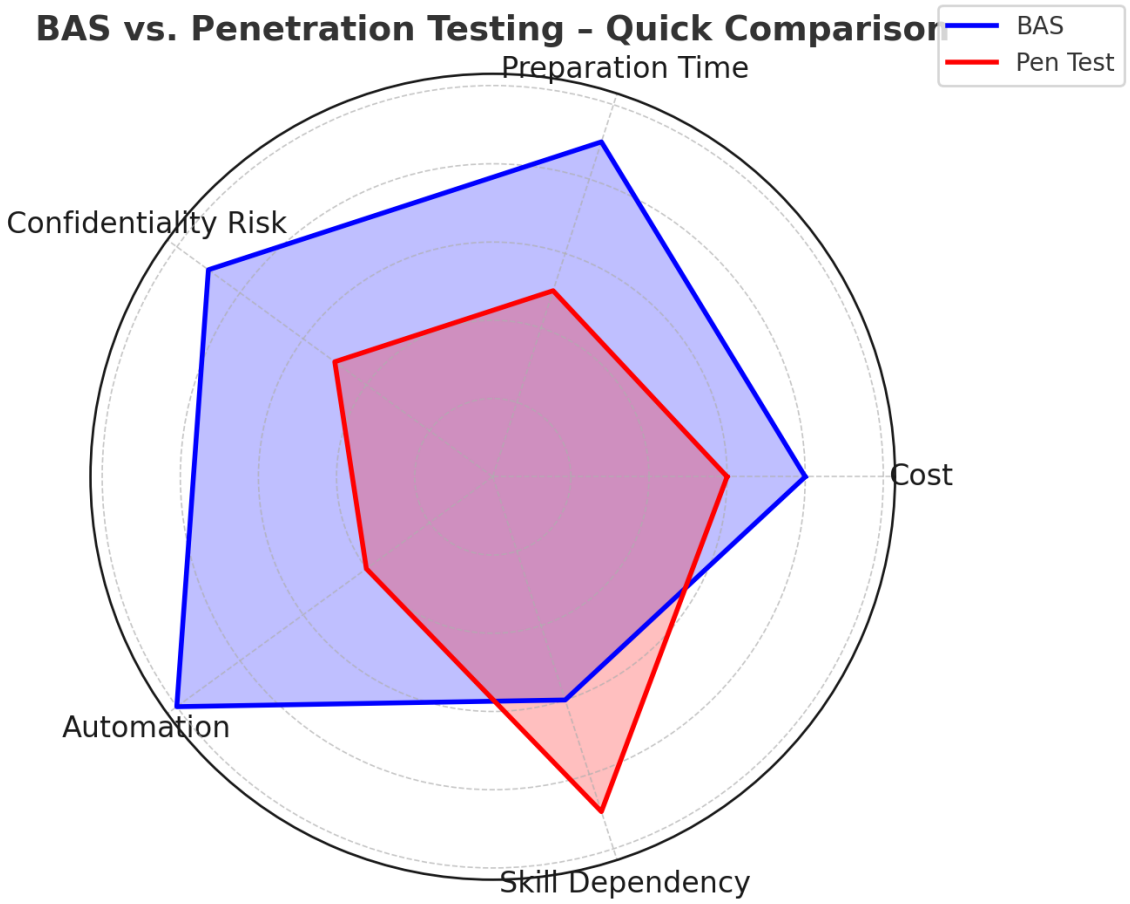

Breach Attack Simulation vs. Regular Penetration Testing

This report provides a comprehensive comparison between Breach Attack Simulation (BAS) and regular penetration testing, covering differences in methodology, cost, preparation time, legal considerations, and potential confidentiality risks. Examples, common tools, and visual charts are included for clarity.

1. Overview of the Two Approaches

• Breach Attack Simulation (BAS): BAS platforms continuously simulate real-world cyberattacks in a safe and controlled environment, providing automated and repeatable tests against security controls.

• Regular Penetration Testing (Pen Test): A human-led or partially automated process that identifies vulnerabilities in systems, networks, and applications, often with manual exploitation techniques.

Creative Cyber Consulting LLC
Yasser.Alkroasihi@CreativeCyberConsulting.com

2. Cost Comparison

Penetration testing is generally more expensive per engagement compared to BAS, which operates on a subscription or licensing model.

• Average Cost of Penetration Testing: $10,000 – $50,000 per engagement (depending on scope and complexity).
• Average Cost of BAS: $20,000 – $80,000 annually (continuous testing with multiple attack scenarios).

3. Time to Prepare and Legal Considerations

Penetration testing requires significant preparation, including defining scope, obtaining legal approvals, and coordinating with internal teams. BAS typically has a shorter setup time and fewer legal hurdles, as attacks are simulated without affecting production environments.

• Pen Test Preparation Time: 2–6 weeks (including scoping and legal documentation).
• BAS Setup Time: 1–2 hours (mostly technical configuration).

4. Confidentiality Risks

In penetration testing, there is a higher risk of sensitive data exposure, especially if real exploitation occurs. BAS reduces this risk by simulating attacks without actually exfiltrating data.

Example:
• Pen Test – Exploiting a database may expose real customer data.
• BAS – Simulates the attack path without retrieving actual confidential information.

5. Common Tools

• Breach Attack Simulation Tools: Horizon 3, Cymulate, AttackIQ, SafeBreach, XM Cyber.
• Penetration Testing Tools: Metasploit, Burp Suite, Nessus, Nmap, Cobalt Strike.

6. Comparison Chart

Criteria	Breach Attack Simulation (BAS)	Penetration Testing	Notes
Cost	Annual subscription ($20k–$80k)	Per engagement ($10k–$50k)	BAS is cost-efficient for continuous testing
Preparation Time	1–2 hours	2–6 weeks	Pen test requires legal approval
Confidentiality Risks	Low – simulated	Medium to High –	Depends on scope

Creative Cyber Consulting LLC
Yasser.Alkroasihi@CreativeCyberConsulting.com

	attacks	real exploitation	and execution
Automation	High	Medium to Low	BAS is continuous, Pen test is point-in-time
Skill Dependency	Lower (platform-driven)	Higher (expert testers)	Pen test relies heavily on tester skill

7. Conclusion

While penetration testing remains critical for in-depth, human-driven assessments, Breach Attack Simulation provides a scalable, continuous, and lower-risk way to validate security controls. Many organizations choose to implement both, using BAS for ongoing monitoring and pen tests for periodic, high-assurance validation.