SPECTEROPS
Creators of BloodHound

SERVICES

Penetration Testing

Identify Critical System Issues and Attack Paths

Why SpecterOps

Our experience across hundreds of government, defense industry, financial, and healthcare environments has taught us that **the most vital component of a robust security posture is understanding how adversaries will operate against the organization's enterprise environment**. Our objective, across all engagements, is to train and arm our clients with the knowledge of how the effective use of the interlocking components of their security program provide a robust security posture and readiness against sophisticated attacks.

SpecterOps employs and develops our consultants to demystify adversary tradecraft and share their findings beyond our client work. We often release tooling that allows folks to educate themselves on the concepts we talk about—tools like BloodHound, Mythic C2, and Ghostwriter are in every offensive providers' arsenal. **When we say leaders in offensive security, we mean it.**

Why Now

Penetration Testing validates the effectiveness of your organization's preventative security controls and understands what an attacker can do in your environment.

Benefits

- **Assess your organization's ability to prevent attacks in your organization**
- **Identify attack paths that can be chained together to compromise your data and most critical assets**
- **Experienced and unbiased third-party perspective of how adversaries can leverage weaknesses to gain access to your organization**

Our expert assessment will demonstrate the potential impact of a breach and evaluate how effective security controls work to protect your most critical assets. We'll find what automated tools cannot.

Every engagement starts with a simple question—what are you trying to protect? From there, we design your engagement to find issues and attack paths that allow attackers to gain access to your most critical data and assets. By doing so, our team is able to provide the most value with the time you choose to spend with us.

We then move to executing the test by evaluating common attack avenues and moving to less common as the test goes on. SpecterOps consultants are often at the forefront of researching and authoring tradecraft, which we will thoroughly evaluate during our engagements, along with many of the industry techniques that adversaries use as well.

Finally, our deliverables will provide comprehensive detail on both successful and unsuccessful attempts at achieving the penetration test objectives. We ensure that our clients understand the tradecraft and techniques that were used during the engagement. **Our recommendations will be tailored and specific so you do not have to wonder what the next step is to close the gaps we find.**

We Focus on Impact Objective Driven Testing

Network Penetration Testing
Assess the effectiveness of enterprise environment defenses against advanced adversaries attempting to gain access to sensitive data and resources through internal or external attack vectors.

Application Penetration Testing
Assess the effectiveness of the application stack's defenses against advanced adversaries attempting to gain access to sensitive data and resources through authenticated and unauthenticated attack paths.

Specialty Technology Penetration Testing
Evaluate the defensive capabilities of complex, specialized, and cutting-edge technology stacks in securing critical assets and detecting advanced attacks.

Independent Expert Perspective
All our penetration testing services are designed to provide a technically experienced, unbiased, third-party perspective of the security posture presented by in-scope systems.

Email info@specterops.io ›

Learn more at specterops.io ›

Real Results

- **Expert security resources:** Our experts, who themselves have discovered the tradecraft in many cases, will be the ones evaluating your program.
- **Real-world breach exercise:** The assessment goes beyond just identifying vulnerabilities, and instead identifies attack paths, simulating the impact and potential consequences of a real-world attack.
- **Enhanced understanding of security control effectiveness:** You'll gain insights into how well your existing security controls are working to protect your critical assets.
- **Comprehensive and actionable reporting:** Understand the attacks that took place, the detection and response gaps, and actionable next steps to improve your defensive capabilities.
- **Transparent and clear communication:** Fully understand the attack paths, vulnerabilities, and areas for improvement.