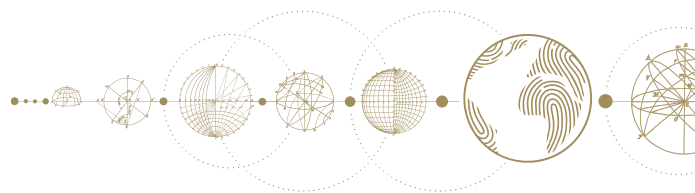# Drummond Security Services
Penetration Testing

Is your organization in need of a Penetration Test?

Drummond and our team of highly qualified security professionals can help. We will identify the key threats to your organization, the assets that are at risk, and the malicious entities attempting to compromise them. Our team of experts employ a trusted methodology and advanced techniques to help identify and exploit network-layer and application-layers vulnerabilities, such as software and system configuration flaws, programming flaws, operational security gaps, and inadequate defensive technology.

Drummond's methodology goes far beyond simply deploying automated tools and technology. It includes human intervention, expert knowledge, and manual exploitation allowing us to best simulate a real world attack. By implementing sophisticated penetration tests, you can confidently secure your data and your customers' data from advanced persistent threats and malicious attacks.

When it comes to any of our Security and Penetration Testing engagements, we do not take a "one size fits all" approach. Drummond understands that every organization has unique technical environments, operational challenges, and varying levels of security program maturity. Whether you require a Penetration Test to be performed as a result of a compliance mandate, or you are following security best practices, we make sure to understand your organization's goals, your technical environment, the critical assets to be protected, and the expected deliverables of the engagement.

The Penetration Test at its core includes the following:
- Vulnerability Assessment
- Exploitation

Additionally, the following services may also be included:
- Authenticated Scans/User Privilege Escalation
- Password Cracking
- Network Security Architecture Assessment
- Social Engineering
- VoIP Assessment
- Wireless Assessment
- Database Assessment
- Quarterly Vulnerability Scans

The results of Penetration Test will include actionable recommendations to help guide and determine the appropriate management action and priorities for managing technical information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

Upon completion of a Penetration Test, you will be provided with a detailed report that includes an overall risk rating based on a proven and well-known threat vector analysis. The overall risk rating will take into consideration the vulnerabilities identified, systems impacted, vulnerability risk score, complexity of compromise, possible attack vectors, and remediation steps. The reports are designed to help your management understand the severity, ease, and business impact of exploitation.

Experience the Drummond difference.

Be prepared and achieve compliance for regulatory information security mandates. Test critical business applications for standards conformance and interoperability. Increase trust, gain expertise and experience our proven methodologies and attention to detail as we partner with you for your long-term success.

With over 20 years of experience, we offer a comprehensive suite of services to help you achieve compliance with complex regulatory information security mandates including HITRUST, HIPAA, PCI, SOC, ISO 27001, NIST and GDPR.

Drummond offers personalized services that are proven to help you strengthen your security posture. Our team of highly skilled experts is ready to collaborate with you and your team.

To get started, please visit: www.drummondgroup.com

DRUMMOND