Penetration Testing

Overview

Penetration is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit. As part of Arete's penetration testing process, Arete's engineers attempt to breach the logical, physical, and administrative controls of their client's infrastructure and note deficiencies in those controls. Arete uses real-world techniques and knowledge cultivated from years of experience to identify and exploit vulnerabilities that could result in a breach of an organization's security. We explore the footprint, enumerate all attack vectors, and attempt infiltration. Our tailored recommendations and reports help clients to better defend their infrastructure against hackers and other malicious attackers. Arete adheres to ethical codes of conduct and will work diligently to help organizations maintain the
confidentiality, integrity, and availability of their information systems every step of the way.

Web Application Penetration Testing

It is important to perform web application testing to evaluate the security of an application; web application penetration activities focus on application weaknesses, technical flaws, and/or vulnerabilities. Areas of web application testing include:

Activity	Description
SQL Injection Testing	SQL injection (SQLi) is a form of security exploit where the attacker would add SQL code to a Web form box to gain access to resources or even make changes to data. Arete tests client websites for SQLi vulnerabilities.
Forceful Browsing	Arete attempts to discover directories and files by appending known or standard files to the URL.
HTML Review	Arete reviews the HTML source code of client Web pages to identify any comments, hidden form variables, or directory names, that may provide useful information for an attacker.
Administrative Interface	Arete attempts to locate known administrative interfaces based on known information, and manually enter the directory and port of default administrative sites
Error Handling	Arete analyzes all error, debug, or exception messages originated from the web server or database for information that may be useful to an attacker.

Network Infrastructure Penetration Testing

Network infrastructure penetration testing is a critical part of your cybersecurity strategy. It should done periodically, it assesses what parts of your network infrastructure are vulnerable to unauthorized access, attacker pivot, and exploitation. Arete's network infrastructure testing includes:

Activity	Description
Enumeration	Arete performs an automated test on all identified interfaces to determine the disposition of any active services allowing connections to an organization's host.
Vulnerability Mapping	Arete analyzes all open ports and services available from organization owned IP address blocks to determine service type, version, and whether any vulnerabilities are known for a particular service.
Penetration Testing	Should a vulnerability be discovered from scanning, Arete attempts to exploit using automated tools and manual processes.
Reviews & Recommendations	Once all testing activities have been completed, Arete generates a report that provides detailed information about all of the activities described above, along with all results of testing.

Our Services

We provide services to a wide range of industries including, financial services, healthcare, non-profits, the federal government, in

surance, journalism & news, retail, technology, education and more. Our clients recognize our team of experts as leading providers of Information assurance services.

- Network Security
- Monitoring Active
- Defense Incident Response
- Digital Forensics Security
- Assessment Security Policy Review
- Social Engineering Information
- Assurance Risk Audits/Assessments
- Custom Software/Hardware Penetration
- Testing Education & Training

About Arete

Arete Incident Response has assembled an elite team of cybersecurity experts to create unparalleled capabilities to address the entire cyber incident life cycle, from incident response readiness assessments to post-incident remediation. Our core skills include triage, digital forensics, malware reverse engineering, remediation, and testifying expertise. Arete works with your organization to provide highly customized advice specific to your business size and industry.

Arete's advisory services provide legally defensible, compliant cyber strategies that assist the C-Suite and Boards of Directors to continuously improve the organizations' cyber posture. Arete partners with clients to reduce the burden of preparing for, detecting, and responding to cyber-attacks. Data breaches are a matter of when, not if in today's world. Engaging Arete's team of experts gives your organization the confidence to respond to a data breach with access to the world's leading cybersecurity professionals – anywhere in the world – within hours not days.