PENETRATION TESTING

GRA QUANTUM

An Assessment with Zero Blind Spots

For a pen-test to be effective it needs to be complete. Our suite of services leaves no stone unturned, examining vulnerabilities emanating from multiple points of entry: from inside and outside your network, from human and technical weak points, and from technical and physical sources.

Network Penetration Testing

Execute a traditional survey of vulnerabilities exploitable by outside hackers and malicious insiders.

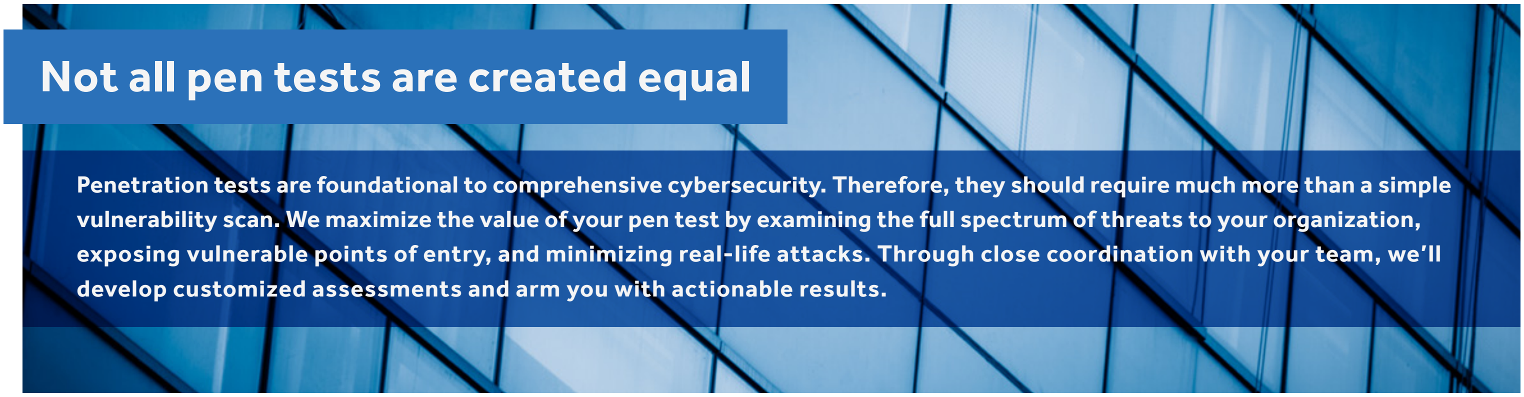
Typical testing entails:

- Automated and manual attempts to gain access to confidential data
- Demonstrations of an attacker’s ability to gain administrator or elevated access privileges
- Local system interrogation and data gathering
- Reconnaissance of nearby hosts
- Formulation and issuance of database queries to key database servers
- Generating actionable recommendations to alleviate or mitigate the issues identified

Wireless Penetration Test

Discover whether known and unknown wireless devices can serve as jump points into your network.

Assessments identify beaconing clients, rogue access points, and the types of encryption deployed around your network. They then attempt to penetrate wireless systems through attacks against the access those pre-identified points.



Not all pen tests are created equal

Penetration tests are foundational to comprehensive cybersecurity. Therefore, they should require much more than a simple vulnerability scan. We maximize the value of your pen test by examining the full spectrum of threats to your organization, exposing vulnerable points of entry, and minimizing real-life attacks. Through close coordination with your team, we’ll develop customized assessments and arm you with actionable results.

PENETRATION TESTING

Application Layer Penetration Testing & Source Code Review

Hire an extra set of eyes to carefully review the security of your new application or program.

Application Layer reviews include testing input validation controls on all data passed from the client to the application, application configurations, and authentication/access control mechanisms. These inspections can include web-based applications, web services, mobile applications, and client-server applications.

Source Code Reviews include automated static and dynamic analysis, and followed up with manual examinations to identify any additional issues, such as business logic and proper use of encryption. We work with the following languages:

- Java and .NET
- C/C++ (Windows, Linux and Solaris)
- Web (J2EE, ASP.NET, Classic ASP (including VBScript and VB6), PHP, Cold Fusion, Ruby, JavaScript (including JQuery and Node.js)
- Legacy Business Applications: COBOL
- Mobile Platforms: Objective C for iOS, Java for Android & J2ME for BlackBerry, JavaScript frameworks including PhoneGap, Apache Cordova, Appcelerator Titanium

Site Security & Social Engineering Penetration Testing

Go beyond the virtual and examine physical security flaws and poor employee practices that may also leave you vulnerable to unauthorized access.

Physical Security inspection will review:

- External and internal perimeter vulnerabilities (e.g., security camera placement, badge readers, and security personnel locations)
- Sensitive data disposal policies
- Employee security awareness

Social Engineering assessment will conduct:

- Telephone and email-based phishing attempts against potential key targets (e.g., human resources, helpdesk personnel, application administrators, general employees, etc.)

World-Class Talent at Your Disposal

Our team of highly-trained experts has decades of experience studying network vulnerabilities and battling hackers. We hail from Fortune 50 firms, law enforcement and intelligence agencies. We bring a wealth of experience serving both domestic and international firms across several industries.

GRA QUANTUM

graquantum.com | info@graquantum.com