Penetration testing identifies organizational weaknesses the same way an attacker would—by hacking it. This enables organizations to better understand and ultimately minimize the risk associated with IT assets.

Today, creating a truly secure IT infrastructure requires access to highly specialized knowledge, intelligence, and expertise in order to stay at least one step ahead of the evolving risks. Because Praetorian is an authority on information security, your business can leverage our subject matter expertise to solve these challenging business problems.

Praetorian offers a wide range of penetration testing services designed to meet your specific needs:

**External Penetration Testing**
Praetorian identifies and examines vulnerabilities for external, Internet facing systems to determine whether they can be exploited by an attacker to compromise targeted systems, or used to gain access to sensitive information.

**Internal Penetration Testing**
Praetorian identifies and examines vulnerabilities for internal, Intranet systems to determine whether they can be exploited by an attacker to compromise targeted systems, or used to gain access to sensitive information.

**Application Penetration Testing**
The overall goal of an application penetration test is to uncover software vulnerabilities, demonstrate the impact of the weaknesses, and provide recommendations for mitigation. During a penetration test, Praetorian has two primary objectives: the obtainment of unauthorized access and/or the retrieval of sensitive information.

**Mobile App Penetration Testing**
Using a combination of manual and dynamic analysis along with custom automated fuzzing, Praetorian’s Mobile Security Testing covers areas such as storage protection, transport protection, authentication, authorization, session management, data validation, and error and exception handling.

**Key Benefits**
- Obtain an accurate understanding of your security and risk posture
- Comprehensive reporting, relevant to your organization and stakeholders
- Comply with industry regulations and information security best practices

**Service Offerings**
- External Penetration Testing
- Internal Penetration Testing
- Application Penetration Testing
- Mobile App Penetration Testing
- Product Penetration Testing
- Wireless Penetration Testing
- Social Engineering Testing

**Trusted by Today’s Leading Organizations, Including:**
- Palo Alto
- SolarWinds
- AT&T
- Johnson & Johnson
- McAfee
- Marathon Oil
- IBM
- Bank
**Product Penetration Testing**
The overall goal of a product penetration test is to uncover software vulnerabilities, demonstrate the impact of the weaknesses, and provide recommendations for mitigation.

**Social Engineering Testing**
Social engineering is commonly defined as a technique that uses persuasion and/or manipulation to acquire unauthorized access. While email phishing is more prevalent, telephone and physical social engineering campaigns can also be used to induce human reaction.

**ATM Penetration Testing**
ATM platforms offer a unique attack surface that requires a multi-disciplinary approach to testing methodologies that incorporates all aspects of the device under test including: physical access, local peripheral access, network surface, and software interfaces.

**Wireless Penetration Testing**
Praetorian’s wireless penetration testing and assessment services evaluate the security of your organization’s wireless implementations and provide recommendations for improvement.

**Phishing Campaign Testing**
A simulated phishing campaign test establishes a phishing attack vulnerability benchmark as well as a structured, on-the-spot user awareness training where employees learn how to help keep the organization safe and secure.

**READY TO GET STARTED?**
Contact us at 1 (800) 675-5152 to learn how Praetorian security services can help you accomplish your specific business and IT goals, or explore more by visiting:

www.praetorian.com

**ABOUT PRAETORIAN**
Praetorian is a full-service information security consulting firm specializing in security assessments, application security, penetration testing, policy development, regulatory compliance, security research, and security training.

Its consultants come from a wide range of backgrounds and specialties. Previous employers include Symantec, McAfee, MIT Lincoln Labs, Rapid7, Sun Microsystems, Dell, IBM, Cisco, Morgan Stanley, Citi, National Instruments and PricewaterhouseCoopers.

The team members include published authors, patent holders, open source developers, industry researchers, and conference presenters.