

## PENETRATION ASSESSMENT

Ignyte Services provide solutions to help organizations effectively manage their security frameworks in environments where threats evolve at escalating speeds.

Our Penetration Assessment offering is a focused and targeted “hacking” attack simulation to identify, evaluate, and demonstrate particular vulnerabilities in your network.

### Penetration Assessment

Ignyte Services’s Penetration Assessments adhere to the **OSSTMM penetration testing methodology** and code of ethics for all of its penetration testing activities. Our security analysts are certified security practitioners holding at least one certification of Certified Information Systems Security Professional (CISSP).

Penetration tests can range in a number of varieties from testing one application based on known vulnerabilities to far reaching tests where no vulnerability information is provided and every system and network is in scope. Additionally, a penetration can go as far as to gain control of the system by any means (aggressive) or to simply illustrate that it “could” be done by “taking these next steps”, without taking the steps.

*Our assessments answer these questions:*

- **Is the present internal control framework sufficient to mitigate risks associated with both internal and external threats?**
- **Can the host systems, applications, or infrastructure elements be compromised – thus adversely affecting the ability to continue business operations?**
- **Are the fundamental administrative procedures, physical safeguards, and technical safeguards in place to protect the corporate image and customer’s private data?**

### Project Initiation – Confirm Objectives & Targets

#### Phase I: Discovery

- Map out Vulnerabilities

#### Phase II: Demonstrate that the vulnerabilities exist

- Test the Incident Response

#### Phase III: Actual exploitation of a vulnerability in a network, system, or application. Obtain privileged access, exploit buffer overflows, SQL injection attacks, etc. This level of test would carry out the exploitation of a weakness.

#### Phase IV: Restoration

#### Phase 5: Project Reporting

### Focused on Results

Our reports provide a thorough analysis and summary of vulnerabilities identified and recommendations for developing the appropriate remediation strategy.

### Solving Enterprise Risks Through People, Process, and Technology

Businesses often discover that buying and installing new security software is only a small part of an enterprise security solution. An effective security solution is one in which an organization manages risk, provides effective processes and implements technology for security enablement. Ignyte tailors the approach to meet your specific business requirements to protect your enterprise resources and ensure business continuity.

### For more information, please visit:

[www.ignyteplatform.com](http://www.ignyteplatform.com)

or call:

1.833.IGNYTE1

### ABOUT INGYTE

Ignyte is a leader in collaborative security and services integrated GRC platform for global corporations. For corporate risk and compliance officers who depend heavily on the protection of their resources, Ignyte is the ultimate translation engine for simplifying compliance across regulations, standards and guidelines.

© 2018 MAFAZO LLC dba Ignyte Assurance Platform. All rights reserved. Published in the USA. 06/18. MAFAZO LLC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.