

## **Penetration Testing**

Today's Cyber threats are higher than ever and news of corporate and government compromise is a regular occurrence. Unfortunately, Firewalls and Antivirus software alone are not enough to keep unwanted intruders out of your network. Current corporate and government networks are threatened by loss of revenue, public embarrassment, and data leakage such as customer financial and personal information. The enterprise environment is constantly threatened by malicious groups, hackers, and even internal employees. Many of these threats can be minimized with proper security assessments.

CGI's Enterprise Penetration Testing provides a comprehensive suite of penetration testing services that identify, analyze, and mitigate an organization's security risk. Through our Penetration Testing service, enterprise weaknesses are identified and recommendations are made to mitigate further compromise. CGI's Cyber security experts can provide external and internal penetration tests, aimed to provide a complete and exhaustive analysis of your enterprise security.

### **External Penetration Testing**

An external penetration test assesses the enterprise border systems and internet ingress points to your enterprise infrastructure for vulnerable links in the chain. Such weaknesses could be used by external attackers to disrupt the confidentiality, availability, and integrity of the network. The result of this comprehensive analysis allows the organization to address each weakness, and secure the infrastructure.

### **Internal Penetration Testing**

An Internal Penetration Test reveals weakness in the network from the perspective of an employee or consultant who possesses some level of trusted access to your infrastructure. An internal assessment shows how the insider threat may compromise the network, gain access to confidential data and cause damage to your IT infrastructure. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network. This type of assessment allows the organization to address vulnerabilities before they are exploited.

### **Components of Penetration Testing**

- Scoping & Rules of Engagement
- Analysis & Identification of Attack Vectors
- Exploit Testing and Penetration Attacking
- Immediate Notification of Critical Risks
- Business specific & Technical threats and Recommendations
- Exploitation Results organized by Risk and Areas of Concern
- Details and Exposure of Vulnerabilities
- Strategic and tactical remediation plans