

## Vulnerability Assessment

The biggest fear of any organization responsible for protecting its intellectual property or other customer data is a data breach that could have been easily prevented if previously identified. CGI's vulnerability assessment teams conduct comprehensive scans of the internal and/or external networks to identify potential vulnerabilities which could leave their organization open to an attack. Our teams use the latest tools and techniques already being successfully used "in the wild" by attackers against other organizations. Findings are presented in a clear and concise fashion categorized by severity and level of effort to perform the corrections to the infrastructure. These assessments when conducted quarterly to annually ensure potential security risks are identified in a timely manner and also demonstrate due diligence to leadership and customers to protect its sensitive information and customer data.

## Internal Assessment

While the best information security professionals in the business can implement strict processes, procedures, and protocols for managing information assurance and mitigating the inherent risks and threats of operating in the digital world of today, the one thing that will always be a step ahead is the pace of government operations. Internal assessments can be performed from within three general scenarios.

- A "No Knowledge" scenario. This is designed to simulate an external attacker gaining access to the enterprise by means of either a social engineering attack or a successful external to internal penetration.
- A "Partial Knowledge" scenario. This is designed to simulate either an attacker who has already performed reconnaissance on the network and has an idea of what to attack, or a disgruntled inside employee looking to access resources that would have otherwise been restricted.
- A "Targeted Assessment". This is designed to only assess specifically requested network nodes and segments. Typically identified as a high value target.

## External Assessment

External enterprise security, or perimeter security, is one of the most difficult challenges an enterprise security team faces. Not only do the perimeter devices such as routers and firewalls need to withstand the constant barrage of attacks delivered by automated Trojan bots, "script kiddies", and criminal enterprises, but they also need to withstand the vulnerabilities inherent in the third party software and services employed by the government which have unknowingly created points of entry into the enterprise. Attackers are aware of these vulnerabilities and have scripted specific attacks to leverage these weaknesses allowing them to scan large ranges of the internet for vulnerable corporations. These identified vulnerabilities aren't always immediately exploited. In some cases a list of entities with these identified vulnerabilities are compiled and then sold to more nefarious operations.

External assessments can be performed from within three general categories just as the internal assessments:

- A **"No Knowledge"** scenario. This is designed to simulate an external attacker performing scans against the external perimeter as a whole in hopes of identifying a potential point of entry.
- A **"Partial Knowledge"** scenario. This is designed to simulate an attacker who has completed an external reconnaissance operation, or a disgruntled employee looking to access resources that would have otherwise been restricted.
- A **"Targeted Assessment"**. This is designed to only assess specifically requested network nodes and segments. Typically identified as a high value target.

## Reporting

All the technical capabilities and processing power in the world are useless if at the end of the analysis the findings cannot be put together in an intelligent manner that not only provides a clear and concise understanding of the findings. At the end of the assessment findings are presented in a clear and concise fashion categorized by severity and level of effort to perform the corrections to the infrastructure.