# Vulnerability Assessment and Penetration Testing

Framatome's Vulnerability Assessments identify and quantify vulnerabilities, and provide recommendations to eliminate or mitigate the risk. Our Penetration Testing uses advanced hacking techniques to safely simulate attempts to gain access to your infrastructure, and results in recommendations to better protect your networks and systems from compromise.

Framatome's Vulnerability Assessments identify and quantify vulnerabilities, and provide recommendations to eliminate or mitigate the risk. Our Penetration Testing provides another set of information by simulating covert and hostile attacks against your infrastructure to test your system against advanced hacking techniques and to determine what can be attained.

## Vulnerability Assessments

Vulnerability Assessments include identification of key assets and resources, prioritization and quantification of the value of these assets and resources, identification of the vulnerabilities of these assets and systematically eliminating or mitigating the risks for the most critical assets or resources.

## Penetration Testing

Framatome's senior security engineers use "best-in-class" scanning tools to simulate real-world attacks and mimicking the tactics employed by malicious hackers. We then identify which vulnerabilities present the highest potential risk to your environment. The result is a comprehensive report with risk-rated findings and recommendations to better protect your networks and systems from compromise.

**Step 1:** Discovery — Our experts conduct methodical reconnaissance, scanning, and reporting to discover, verify, and report security flaws. From the Internet to inside your company, what are the weakest links in your chain?

**Step 2:** Attempted Exploitation — Suspecting a weakness and proving one are two different things. One a theory; the other, something that cannot be ignored. In close coordination with your organization, our team will use a variety of tools and manual techniques to leverage the discovered weaknesses and prove the ease of actual penetration. Carefully recording our steps, theory becomes reality.

**Step 3:** System Compromise — Often infiltrating the system is not enough. Can anything harmful or destructive be done? Our professionals will work with you to identify your critical data and systems. After establishing our presence, be it in your email server or the HVAC controller, we attempt to capture your critical data and validate the weakness.

**Step 4:** Debrief and Recommendations — Once completed, our team provides a complete description of our efforts and an executive summary suitable for leadership understanding. We provide advice on remediations and improvements, and we stand by to share our knowledge on how to strengthen defenses.

framatome

## Testing Protocols

Common testing procedures include discovery, research, exploitation and documentation. Framatome's elite testing team will identify Operating System versions, network devices and configurations, and applications. Research is performed to identify vulnerabilities on the systems you implement.

Brute force attack methods including: password cracks, buffer overflows, string formatting errors, SQL injection, and cross site scripting may also be employed to attempt to compromise and gain access to your organization's information resources. All procedures will be documented to provide you with a clear understanding of what was discovered and the level of compromise obtained if successful.

## Why Framatome?

Framatome has a long history of providing cyber security solutions, including vulnerability assessments and penetration testing, to the nuclear industry as well as other commercial clients. Our testing approach has been proven successful in the energy industry and our highly experienced team is provided at a very competitive price.

Our project team has decades of technical experience and the innovative thinking that is necessary to successfully perform penetration testing with the highest quality and technical excellence. By using our real-world experience gained from previous development, operations and audit engagements, our experts provide results that are relevant and actionable. We align our efforts with the critical elements of your business. We deliver high-quality results, quickly, and with minimal impact on your resources and personnel.

**Framatome Inc.**
**Corporate Headquarters**
7207 IBM Drive
Charlotte, NC  28262

For more information, contact:
**Nick Kim**
Cyber Security and I&C Design Engineering Supervisor
Tel: 704.805.2743
Cell: 980.266.1191
Nick.Kim@framatome.com