# Securing Your Critical Infrastructure

## Network Penetration Test

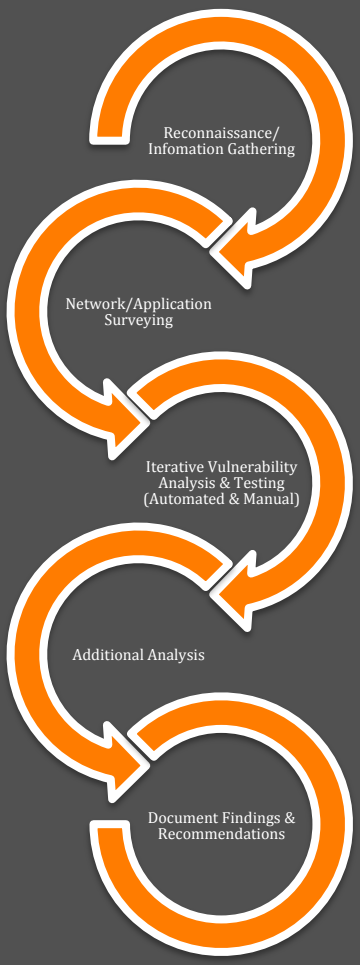
- PINPOINT NETWORK AND SYSTEM SECURITY FLAWS
  Determine whether the networks and systems are resilient to unauthorized access or malicious attacks and afford adequate protection.
- ASSESS NETWORK SECURITY ARCHITECTURE
  Determine whether the network architecture is adequately configured to mitigate probable attack vectors, as well as afford client's sufficient knowledge and notice to adequately respond to any attack.
- ASSESS EXISTING PROCESSES AND PROCEDURES
  Analyze whether existing processes/procedures are adequate to prevent a reoccurrence of vulnerabilities.
- ANALYZE AND DOCUMENT FINDINGS
  Analysis and documentation, including findings and recommendations at both a technical and procedural level.

relay SECURITY GROUP

## Service Offering

### Details

Relay Security Group, LLC (Relay) was founded in 2007 by information security professionals with over twenty years of cumulative IT security experience in a wide range of markets. Our mission is to provide our clients—through actual validation of vulnerabilities and with minimal impact on their often-sensitive operations—with the most accurate information about security threats to their environments and their readiness to meet current industry standards and regulations. Relay's validation methodology, processes, and recommendations take into account the complexities of these environments, which translate to recommendations that are both reasonable and actionable.




Relay's Network Penetration Testing services are based on proven penetration testing and vulnerability assessment methodology, which incorporates the Open Source Security Testing Methodology Manual (OSSTMM) v3.0 in combination with Relay's proprietary techniques that, not only takes into account industry specific requirements, but also provides a detailed review of the client's systems and networks. In addition, our methodology also helps identify inter and intra-system trust relationships for critical systems/networks within the infrastructure that can pin point single points-of-failure in an otherwise secure environment.

The testing consists of a focused process of finding and validating vulnerabilities, as well as determining how they indirectly or directly impact the environment. The penetration test is conducted either externally (from the Internet) or internally (from the corporate environment) and can be either a blind (without prior knowledge) or cooperative (with specific information) effort. In either case, all intrusive testing will be conducted with the cooperation of the client, so as to minimally impact the infrastructure. No attempts are made to harm or cause degradation to any system or network, but merely to demonstrate capabilities of compromise for validation purposes.

In brief, the network penetration test will assist a client in determining:

- Detailed understanding of the types and impacts of attacks against the infrastructure, including potential attach paths and scenarios;
- Deficiencies in the information security and risk posture for both the external and internal networks and systems;
- Deficiencies in the implied and formal documented policies and procedures;
- What the overall operational and business impacts are due to the discovered information security issues; and
- The most reasonable and expedient path to address these issues at a business, technical, and operational level.

3750 Brodie Way Dublin California 94568 ☎ 800.613.0431 ✉ sales@relaysecurity.com WWW.RELAYSECURITY.COM