

PENETRATION TESTING

While many organizations may be aware of system or network vulnerabilities, a surprising amount never perform “proof of concept” testing by simulating an attack from a malicious source. Given today’s growth in breaches and other attacks, an active analysis - carried out from the position of a potential attacker - of system configurations, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures - is clearly needed.

Through active penetration testing, *Intekras* IT security experts are able determine the feasibility of an attack and the amount of impact a successful exploit, if discovered, may have. Our attack methodologies and vectors can address the following:

- Network Components
- Desktop/Laptop Devices
- Mobile/Wireless Devices
- Database, DNS, and Web Servers
- IDS, IPS, Firewalls, and Proxies
- Web, Email, Web 2.0 and Other Internet-Based Applications
- Social Engineering, Client-Side Attacks, and Brute Force Techniques

Our penetration tests are more than just “ethical hacking”, as they are intended to:

- Identify key information assets that require protection and the potential threats and likely adversaries
- Determine the effectiveness of existing and planned countermeasures for key assets
- Determine the degree of risk of each key asset
- Provide prioritized countermeasure recommendations
- Provide a roadmap of individual countermeasure actions as well as integrated and collective countermeasure costs.

The *Intekras* Penetration Tests are based upon generally-accepted testing methods for detailed reconnaissance, deep scanning, exploitation, pivoting, and management reporting - tailored to maximize the value of testing from a management, technical, and risk perspective. Our testing activities are performed by highly experienced and certified (CISSP, CEH, GIAC) experts who follow testing methodologies as specified by the EC-Council, SANS, ISACA, NIST, OSSTMM, OWASP, (ISC)2, CICA ITAC, and many others.

Intekras utilizes the most current COTS and Open Source penetration testing tools and works closely with security operations personnel to ensure that any critical security issues found are resolved immediately. Additionally, we are able to provide a full risk-ranked assessment of likelihood and impact of an attack and recommended risk treatment (mitigation, transfer, or acceptance).

The result is an extensive analysis that documents and risk-ranks all vulnerabilities found and proven, and that suggests corrective actions, safeguards, and countermeasures. The *Intekras* Penetration Test is a valuable means of evaluating your security and preparing your defenses against the real thing - finding vulnerabilities and fixing them before an attacker does.

