LOWERS & ASSOCIATES
International Risk Mitigation Partners
125 East Hirst Road, Suite 3C | Purcellville, VA 20132

Information Technology Risk Management Services

Vulnerability Analysis Through Penetration Testing

Are your networks or systems susceptible to compromise by a malicious attacker, unethical competitor, or unscrupulous employee? Lowers & Associates (L&A) is able to answer that question through its Penetration Testing services.

What is Penetration Testing? Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. If the focus is on computer resources, then examples of a successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information. The main thing that separates a penetration tester from an attacker is permission. The goal of a penetration test is to increase the security of the computing resources being tested. In many cases, a penetration tester will be given user-level access and in those cases, the goal would be to elevate the status of the account or user other means to gain access to additional information that a user of that level should not have access to.

How Do Penetration Testing and Vulnerability Testing Differ? Penetration testing has more of an emphasis on gaining as much access as possible while vulnerability testing places the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. A vulnerability assessor will stop just before compromising a system, whereas a penetration tester will go as far as they can to identify all areas of IT risk.

How Does L&A Perform Penetration Testing? We take a unique approach to Penetration Testing by mimicking the actions of real-life internal or external attackers:

1. **Footprinting**: Performing reconnaissance by researching public information on the company and targets, including technical listings, on-line news sources, business postings, and many other on-line resources;
2. **Scanning**: Identifying specific systems and services, software and operating system version levels, hardware devices, databases in use, and other information;
3. **Enumeration**: Identifying specific vulnerabilities and avenues of attack through both automated and manual means;
4. **Privilege Escalation**: Exploiting identified vulnerabilities to gain initial access to a system, and attempting to compromise accounts/services with greater authority;
5. **Interactive Control Establishment**: Acquiring true interactive access to a system via a command line, shell, or graphical interface; and
6. **Expanding Influence**: Staging attacks against other target network resources from the compromised box, by leveraging "trusted relationships" between systems.

During our Penetration Testing, we evaluate vulnerabilities separately and - if damage to a system is likely - we will report the vulnerability, but shall refrain from full exploitation. Also, if required, we're able to stage "client side attack"', whereby carefully crafted emails and hyperlinks are sent to ensure that Computer and Internet Use policies are being adhered to, or that browsers are not vulnerable.

The result is an extensive report documenting and risk-ranking all vulnerabilities found and proven, and suggesting corrective actions and countermeasures. The L&A Penetration Test is a valuable experience in evaluating your security and preparing your defenses against the real thing - finding vulnerabilities before an attacker does, and fixing them.