Understanding Penetration Testing

Penetration testing, also known as **pentesting** and ethical hacking, is an evaluation of a system or network using simulated attacks in an attempt to identify security vulnerabilities. Through the techniques utilized in this test, weak points in a system can be identified - and subsequently patched through additional measures - so that there is a reduced risk of an actual breach.

What Causes These Vulnerabilities to Occur?

A **vulnerability** is a weak spot in your network that might be exploited by a security threat. Failing to identify a vulnerability in time may lead to a loss of data, lengthy site downtime, and/or a completely compromised system. Here are some common causes of these vulnerabilities:

- Poorly configured or overly complex system
- Hardware and software design / development flaws
- Lack of secure passwords
- Unsecure network
- Communication security issues
- Failure to keep up with software upgrades
- Poor internal cybersecurity training

Why Should Your Business Get Pentested?

Every organization should make the effort to identify security issues present in their internal network and computers. If yours needs the extra push, consider these additional reasons:

- Determine security vulnerabilities
- Verifying that critical or sensitive data is secure when transferring between systems or over the network
- Assess business impact if an attack is successful
- Help meet information security compliance requirements
- Guide implementing a better network security strategy
- Avoid facing legal issues that occur when sensitive data is compromised

argentum IT

www.argentumit.com
info@argentumit.com
linkedin.com/company/argentum-it

(502) 473-6407
1141 S. 2nd Street
Louisville, Kentucky 40203