External Penetration Test

What is an External Penetration Test?

A CoNetrix Penetration Test helps identify potential weaknesses within your organization, whether structural, technological, or procedural. CoNetrix Penetration Tests are much more substantial than an automated port scan. We offer full Penetration Tests with in-depth testing using multiple tools with different perspectives, as well as testing by security engineers. Our easy-to-read reports show findings sorted by associated risk, and include a detailed review with a CoNetrix security expert.

Who needs a Pen Test?

An external penetration test is best for any financial institution or company with a high-risk system.

According to the FFIEC IT Examination Handbook, "High-risk systems should be subject to an independent diagnostic test at least once a year. Additionally, firewall policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly."

What gets analyzed?

A CoNetrix Penetration Test can analyze the following areas for vulnerabilities:

- Internet connections (scanned quarterly)
- Phone lines
- Scanning for thousands of vulnerabilities
- Perimeter strength using non-intrusive hacker utilities
- Wireless vulnerabilities
- Employee security awareness (Social Engineering)

Social Engineering

Our Penetration Testing service includes the use of social engineering tactics on employees. Employees are targeted at random, the number of which depends on the size of the company.

- Small institutions (20-30 employees total): We attempt to target all employees.
- Large institutions: We attempt to target some (5-10) employees at each location.

The main contact for the Pen Test will receive a copy of the material we send in order to field questions from employees. Social Engineering is included in the price of the penetration test.

Social Engineering Methods

Some of the methods we use include:

Mock Web Sites - We build a mock website that replicates the institution's own website, and conduct two different tests with employees. Our sites do not store any private information and only public information is transmitted back to CoNetrix. All information obtained is included in the report findings.

Spoofed E-mail - We send an e-mail that appears to have been sent from bank management, normally our primary contact. The spoofed e-mail asks users to try the "mock website".

Phone Calls - We call employees and ask them to try the "mock website". The CoNetrix employee placing the calls completes a detailed log to be included in the report findings.

Why CoNetrix?

Knowledge and Expertise:

- CoNetrix has conducted more than 900 different Penetration Test engagements since 2001.
- The CoNetrix staff has more than 500 years of accumulated information technology, network, and security experience.
- CoNetrix's security experts hold numerous security certifications, such as CISSP, SSCP, CISM, CISA, and other Microsoft and Cisco security specialization.

The CoNetrix Difference:

- CoNetrix provides easy-to-read reports with findings sorted by associated risk.
- Reports include a detailed review with a CoNetrix security expert.
- CoNetrix offers comprehensive Penetration Tests, not just simple port scans.
- In-depth testing is performed using multiple tools from different perspectives.
- CoNetrix Penetration Tests are much more substantial than an automated scan. Human perspective, observation, and experience help identify vulnerabilities.

□ **Request a quote**
conetrix.com/pentest

CoNetrix
A Family of Technology Companies