

## Apples and Oranges

Most legitimate information security consulting firms offer various information security assessments, ranging widely in scope and price. Our clients often complain of the difficulty in comparing one proposal to the next. We hope this one-sheet can help clarify the types of information security assessments that are available.



## Terminology

When requesting tests or security assessments, our banking clients sometimes refer to:

- Vulnerability Assessments or IT Risk Assessments
- Penetration Tests, Pen Tests, or Perimeter Tests
- IT Audits, Security Audits
- Network Scans, Nessus Scans

## Penetration Tests and Perimeter Network Scans

The most popular term used by non-security persons is “pen test” or “penetration test.” In the most literal interpretation of this term, a penetration test imitates attack methods used by hackers with a “capture-the-flag” mentality. After the first vulnerability is exploited, this approach only shows that your network can be penetrated. We do not use this approach. Instead, we provide Perimeter Network Scans. The difference between our approach and penetration testing is that we scan your network perimeter against all known vulnerabilities. We still perform these scans “blindly,” meaning that we don’t have any information about your network.. But the goal is to find, analyze, and confirm ALL vulnerabilities, resulting in a risk-based project plan for mitigation.

## Internal Network Scans

To scan your internal network, we install a device on your internal switch (after the blind scanning is finished, of course). This device, called the mole, builds a VPN back to our Network Operations Center which then allows us to scan your internal network remotely. Because scanning can be intrusive, we remotely scan your network in off-hours.

## Analysis and Report

We take pride in our analysis and confirmation process. Approximately 60% of vulnerabilities found by scanning software are false positives, but we confirm all vulnerabilities listed on our report. Our final report includes a high-level, non-technical Executive Summary that can be understood by management and board members. We also provide detailed analysis information for the technical team, as well as metrics and recommendations. The cusp of our report is a Vulnerability Matrix, which presents a list of all vulnerabilities in a risk-prioritized format.

**Ask all of your alternative providers for a sample report!**

## Ancillary Vulnerability Assessments

There are several minor assessments that can be performed to help test certain policies or programs related to Information Security. The following is a list of the more popular services:

### Physical Breach Tests

To test physical access controls and related incident detection and response, testers will attempt to passively breach physical controls, if they exist, and gain access to the network from the inside. We will pose as a member of your network support team, as a telephone repair person, etc. The report describes the attempt at each location and the response, a summary report showing the percent of penetration, and recommendations.

### Password File Analysis and Report

We can either attempt to capture a SAM or password file from chosen systems or the client can provide the file. The password file will be audited for easily crackable passwords. We report the passwords that have been compromised and the timeframe an average attacker would have been able to discover these after obtaining the password file, thus giving a picture of the strength of passwords in place. The purpose of this process is to demonstrate the power, in terms of time gained, of strong passwords as well as measure the enforcement of the bank’s existing password policy.

### Phishing Expedition

We usually send employees an e-mail, spoofing a client employee, that directs users to a duplication of the client’s Website. From there, the employees will be required to reveal sensitive information, such as their network username and password. Our report summarizes percent penetration, shows print-screens of the e-mail and phishing site with annotations pointing out what should have forewarned the user that this was not a legitimate e-mail and/or web site. We also provide the user names and passwords for all users who failed the test. This summary, along with the print screens, are very useful in your information security awareness program.

### Network Architecture Review

We will assess your network security by analyzing the formal architecture specifications, network diagrams, equipment, software, and processes in place. Our report includes a high-level executive summary with recommendations.

### Other Services

We provide other vulnerability assessment services ranging from war dialing, war driving, dumpster diving, telephone attacks, disaster recovery testing, and physical security audits. Let us know your interests!