



Vulnerability Assessment



Assessment Strategies

In the ideal world, the assessment strategy begins before a computer network becomes operational with the individual computers so that no flawed computers are introduced into the network. The network can then be probed for security vulnerabilities. Finally, the external network defense, the firewall, is verified before any connection to a public network is allowed.

In reality, there are often existing computer networks and external Internet connections. This situation introduces a significant number of known vulnerabilities. The tendency is to squander scarce resources on the most prominent vulnerabilities rather than investing the effort on the vulnerabilities that pose the greatest risk to the enterprise.

A comprehensive network security policy including routine vulnerability assessments is essential. Due to the increasing sophistication of intruder methods and the vulnerabilities present in many applications, it is imperative to assess network security.

If through a vulnerability assessment, a network security issue is detected, applying the appropriate security patches in a timely matter is imperative.

1903 Solutions LLC
San Diego (HQ)
Phone: 619.206.7127
info@1903solutions.com
www.1903solutions.com

Is your company vulnerable to a security attack?
A vulnerability assessment can give you critical insight.

The 1903 Vulnerability Assessment is designed to give a company visibility into their Internet attack surface. It will show how the company appears to an outside attacker who has no special access to the enterprise. It evaluates all exposed ports and possible Internet based points of entry. Discovered services and ports will be probed for vulnerabilities including patch level and potentially risky configurations. The report we provide will provide a clear picture of how the enterprise appears to the Internet. All tests are performed as an unprivileged user with no special access.

The test is performed in multiple phases. The first phase is host and subnet discovery. Using public information, the auditor will attempt to determine all of the companies' public networks. DNS information, whois information and router databases will be probed for company networks. Once this is performed, we will verify our findings are complete by comparing it against a customer provided list. Then we will move on to host discovery.

Utilizing a myriad of tools we will scan the defined subnets for accessible hosts and ports. Each discovered port is probed to determine actual service, potential vulnerabilities and tested for insecure configurations. Based upon customer preference actual exploits can be performed however actual exploits may crash the server or service. If safe checks are used then patch level will be determined and used to measure vulnerabilities.

From this data a detailed report including all discovered hosts and ports will be created and provided to the customer. Each discovered vulnerability will be discussed and information on remediation will be included. Insecure configuration will also be discussed with both reasons and risks included. Alternative options will be provided where possible.

Each vulnerability assessment is unique and the end result is largely dependent on each customer's individual environment. All of the results will be presented and discussed with the customer after the assessment is performed. The length of the assessment can vary depending on what we find but we recommend planning on about 3 to 4 weeks from start to finish. However we want to assure the accuracy of our results so we may ask to extend the delivery date.

