

## What is a Vulnerability?

Security holes/bugs are faults, defects or programming errors. These may be exploited by unauthorised users to access computer networks or web servers from the Internet. As these vulnerabilities become known, software publishers develop 'patches,' 'fixes' or 'updates' that you can download to fix the problems.

In the security community, the word "vulnerability" describes a problem (such as a programming bug or common misconfiguration) that allows a system to be attacked or broken into. Culture: Finding vulnerabilities is a big part of the hacker/infosec culture.

Finding vulnerabilities is way of proving that you are "elite". This subculture is similar to the scientific community. For example, there are a number of people (usually commercial companies) that are "research whores": they take existing research and add their own small contribution, but then publish the result in such a way that leads people to believe that they are responsible for all the research leading up to that discovery.

The words exploit and vulnerability are tightly bound together. Often, an script/program will exploit a specific vulnerability. Since most vulnerabilities are exploited by script kiddies, the vulnerability is often known by the name of the most popular script that exploits it. Key point: There exist broad-spectrum vulnerability scanners/assessment-tools that will scan a system looking for common vulnerabilities. These are often used in order to harden a system.

In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak password, software bugs, a computer virus or a script code injection, or a SQL Injection.

A Vulnerability may exist only in theory, or may have a known instance of an exploit.

Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities.

The SecPoint® Protector (<http://www.secpoint.com/secpoint-protector.html>) protects vulnerable servers with many vulnerabilities from Internet attacks.

The SecPoint® Penetrator (<http://www.secpoint.com/secpoint-penetrator.html>) allows the customers to analyse their network for vulnerabilities and weaknesses.