

What is an exploit?

When an attacker identifies a security vulnerability in a software application, for example a mail server, a web server, a DNS server, a ftp server or a firewall system or other devices the goal will be to gain leveraged access on the target system.

There are many types of security vulnerabilities. The most common are buffer overflow and stack overflow. Generally overflow vulnerabilities causes the software application to do something that it is not meant to. In order to exploit these vulnerabilities to gain leveraged privileges on the target system, an attacker is required to write a piece of source code called "an exploit". This will take advantage of the identified security vulnerability and push the software to the limit, breaking it and in the breaking process gaining leveraged access to the target system with the same privileges as the given program that is being attacked.

What is the difference by launching a real attack and doing a vulnerability scan?

Doing a Vulnerability Scan it is harmless process that uses many techniques to identify vulnerable applications on the target system. This could be by relying on version banners from the software, look the presence of the vulnerable files, and identify old non patched software and many more techniques.

However when relying on version banners, presence of known vulnerabilities and other techniques you can not always be 100% certain that a vulnerability is found since that you did not do the physical break in and get the leveraged privileges.

Why is it important to be able to launch a real exploit?

It is important to launch a real exploit against your system in order to determine as close as possible to 100% that all your patches are working and that you are running the latest versions and service packs on your system.

What are the risks of launching a real exploit?

Doing a vulnerability scan which rely on version banners, presence of known vulnerable files and / or other techniques, is a very smooth process that is designed not to harm anything on your system and not to be aggressive at all.

When launching a real exploit even though The SecPoint Exploitation framework has been designed to minimize risks, there will always be a risk of crashing the target application.

It is therefore highly recommend to test all your pre-production systems by launching real exploits at them, so when they go online in a production environment you are ensured the high security of the systems. However it is obviously still necessary to test your production systems as new threats occurs on a daily basis.