

## Penetration Testing:

### What is a Penetration test?

A penetration test subjects a system or a range of systems to real life security tests. The benefit of a complete penetration suite compared to a normal vulnerability scan system is to reach beyond a vulnerability scan test and discover different weaknesses and perform a much more detailed analysis.

The user can perform specified attacks in high detail after the specific choices and needs. This is normally done via many advanced techniques and utilities by a security consultant.

When performing a Penetration test with the SecPoint Penetrator you have the advantage of a wide range of integrated advanced utilities to do Penetration testing. This includes extensive vulnerability scanning, launching of real exploits, buffer overflow attacks, a wide range of advanced utilities and Denial of Service. No matter if you are an end user or a security consultant it allows you to personalize all the reports with the desired logos and text of the user's choice.

### Penetration Testing compared to Vulnerability Scanning:

The advantage of a Penetration Test compared with an automated vulnerability scan is the involvement of the human element versus automated systems. The human can do several attacks based on skills, creativity and information about the target system that an automated scanning can not do.

Several techniques such as social engineering can usually only be done humans, since it requires physical techniques that have to be performed by a human and is not covered by an automated system.

### The penetration test process:

#### Discovery:

The SecPoint Penetrator uses different tools such as information discovery via a wide range of techniques: whois databases, scan utilities, Google information and more to gain as much information about the target system as possible. These discoveries often reveal sensitive information that can be used to perform specific attacks on.

#### Enumeration:

Once the specific networks and systems are identified through discovery it is important to gain as much information possible about each system.

The difference between enumeration and discovery is the state of intrusion. Enumeration is active trying to obtain user names, running software version information, hardware devices.

#### Vulnerability identification:

The vulnerability identification is a very important phase in penetration testing. This allows the user to determine the weaknesses of the target system and where to launch the attacks.

#### Exploitation – Launching of Attacks:

After the vulnerabilities are identified on the target system then it is possible to launch the right exploits. The goal of launching exploits is to gain full access on the target system.

**Denial of Service:**

A Denial of Service test can be performed to test the stability of production systems to show if they can be crashed or not.

When performing a Penetration test of a pre-production system, it is important to test the stability of the system and if it can be crashed so when it is deployed in a real environment the stability will be ensured.

It is important to perform Denial of Service testing to ensure the stability of the systems. If an attacker takes down the systems during busy hours, the customer can incur a financial loss.

**Reporting:**

After the completion of a complete penetration test, it is important to get user customized reporting suites for technical and / or a management overview. This includes Executive Summary, Detailed recommendations to solve the identified vulnerabilities, Official Security ID Numbers for the vulnerabilities. The reports comes in different formats such as Html, PDF, Xml and all the reports are open to be modified as of the user's choice.

