

### **What is a Vulnerability Scanning?**

Vulnerability scanning is an automated security test that scans a target IP address for known and unknown vulnerabilities. This can be a router, firewall, IP telephone, Windows, Linux, Unix etc. When a vulnerability is identified, a detailed remedy is provided so that the end user can rectify the situation.

### **Intelligent Service Detection:**

SecPoint has an intelligent service detection built in so that when you have services running on non standard ports, the system will be able to detect and base attacks against these ports. The end user is then always assured the most accurate and fastest scan.

### **Launch real exploits:**

New in this edition, it is possible for the end user to launch a high amount of real exploits against a target system. When the user launches real exploits it can help to test if the applied patches on the systems are working or not.

### **Denial of Service:**

You can launch a wide range of very intensive Denial of Service for multiple applications such as Web, Mail, Ftp, Databases and more. Extensive Denial of Service can be launched to try to crash the target system.

The advantage of Denial of Service is to test the stability of a pre production system in order to discover potential instability vulnerabilities.

It is also recommended to test the stability of production systems during night time. If an attacker can manage to crash a production system during peak hour this can lead to a financial loss for you or your customer.

### **Scans any Operation System, Operating device:**

The Penetrator is designed to scan any operating system and work its way through the whole process. The Penetrator has a system built in that allows you to launch unknown Buffer Overflow attacks. This allows you to discover unknown vulnerabilities in your applications or in the target system.

### **Automatic Crawl System:**

The Automatic Crawl System will identify SQL Injection, Cross Site Scripting, and Errors in both known and unknown scripts and software on your web server.

### **Advanced scanning:**

The Penetrator allows for advanced customization in each scan. The end user can fine tune values and manually insert Virtual hosts, Unknown directories on the web server, enable aggressive scanning, extended brute force and other features.

In this way The Penetrator can do an even more customer specific scan of the equipment.

It is designed to minimize its own traffic use on your network based on the intelligent scanning.

**Scan Template Creation:**

Via the scan template creation system the end user can create scan templates with the specific configuration needed, and use these scan templates for scheduled scanning or when making a new scan in the future.

This ensures the end user can apply the same policy, and saves time as there is no need to make a new configuration each time.

**Detailed Vulnerability Remediation:**

Detailed remediation information how to apply patches, install new services packs.

All links are always updated via the intelligent SecPoint quality system.

**Advanced Scheduling:**

You can perform schedule based scans based on the templates of a single system or a large range of systems to start at any time of your choice. It is recommended to scan all your systems in the weekend so you always have the status of your security level at the beginning of the week.

**Non Intrusive Scans:**

The scans performed by The Penetrator are based on intelligent determination and is designed for minimal traffic impact on the target system. This makes sure the scan minimally intrusive for the customer.

**SQL Injection:**

SQL injection is a security vulnerability that occurs in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. The Penetrator can find many kind of SQL Injection vulnerabilities so action can be taken to solve this security risk

**Cross Site Scripting:**

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications, which can be used by an attacker to compromise the same origin policy of client-side scripting languages. Attackers intending to exploit cross-site scripting vulnerabilities must approach each class of vulnerability differently.

The Penetrator can find many kinds of Cross Site Scripting vulnerabilities so action can be taken to solve this security risk.

**Distributed Denial of Service:**

Distributed Denial of Service (DDOS) attacks threaten computer networks worldwide. The increase in the number, sophistication and maliciousness of such attacks has been dramatic in the last few years. Traditional means of network protection, such as firewalls and intrusion detection systems, are weak methods for identifying and blocking DDOS attacks.

The Penetrator can find many kind of Distributed Denial of Service vulnerabilities so action can be taken to solve this security risk.