

# Penetrator

Vulnerability Scanning Appliance  
Penetration Testing Capabilities



**SECPPOINT**  
www.secpoint.com

- ✓ Non US based 100% Backdoor Free
- ✓ 9 Scan Profiles, HIPAA, OWASP top 10, Prepare for PCI, Firewall Scan and more
- ✓ Advanced Web Crawler - SQL Injection - XSS - SSL Vulnerabilities
- ✓ Bugtraq ID / Mitre CVE / Ubuntu USN / Microsoft / OSDB
- ✓ Schedule scans daily, weekly, monthly
- ✓ Prevent Hackers To Access Your Server
- ✓ Vulnerability Scanning
- ✓ Vulnerability Assessment
- ✓ 60.000 + Vulnerabilities
- ✓ Launch Real Exploits and Denial of Service Attacks
- ✓ Distributed Scanning Capability
- ✓ Scan any OS or Network device
- ✓ Reports Branding
- ✓ Detailed Remedies for Identified Vulnerabilities
- ✓ Secure Design All Data Stored on Unit
- ✓ Ticket System for full Vulnerability Management



## PREVENT HACKERS FROM ENTERING YOUR SERVERS AND NETWORK.

### Vulnerability Assessment is key to any security strategy

The latest automated hacking tools can inflict damage across a network and across the world in a matter of hours. Understanding the potential vulnerabilities within your system is vital to any security strategy.

#### Vulnerability Assessment

The Penetrator is a Vulnerability Assessment and penetration testing appliance for your network, which comes pre-loaded and ready-to-use out of the box. It is a powerful, easy to use and intelligent security assessment solution.

#### 60.000 + Vulnerabilities

The Penetrator vulnerability database consists of more than 12 years of research. The database has a total of more than 60.000 unique remote vulnerabilities to test for. This database is updated multiple times daily.

#### Launch Real Exploits and Denial of Service Attacks

You can launch real exploits to verify that an identified vulnerability is exploitable. It is also possible to launch real Denial of Service attacks to test preproduction systems for stability.

#### Reports Branding

Branding and personalisation of reports and selling them as a service is permitted.

#### Unique Distributed Penetrator Capabilities

You can connect multiple Penetrators in a distributed network. This gives many unique advantages such as:

- Centralized reporting
- Centralized vulnerability assessment
- Centralized update point

Possibility to audit different locations from a master Penetrator located in another city.

#### Security Auditing of any Operating System or Network Device

The Penetrator is designed to audit any operating system or network device. It is beneficial to audit any device in the network setup to find and rectify any identified vulnerabilities before an attacker can exploit the vulnerabilities.

#### Multi-User Support for Privacy

All Penetrators support multi-user login. This could be used to create different accounts with different targets to audit or resold as (SAAS) to your own customers.

# Penetrator

Vulnerability Scanning Appliance  
Penetration Testing Capabilities

Specifications	Penetrator S7	Penetrator S7	Penetrator S7	Penetrator S7
Height	1 U Rackmount (57 x 52 x 13 cm) Small Form Factor (32 x 29 x 13 cm)	1U Rackmount (57 x 52 x 13 cm)	1U Rackmount (57 x 52 x 13 cm)	1U Rackmount (57 x 52 x 13 cm)
Weight	SFF without packing: 2,5 Kilo SFFwith packing: 3,5 Kilo 1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo
Power Supply	60W power supply AC/DC 90-264V Full Range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range
Environment Temperatures	Operating : 0°C to 40°C Storage: -25°C to 75°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C
Redundant Power Supply	-	-	✓	✓
Dual processor	-	-	✓	✓
Network	6 GbE ports with 2 Bypass Ports	6 GbE ports with 2 Bypass Ports	6 GbE ports with 2 Bypass Ports	6 GbE ports with 2 Bypass Ports
60.000 + Vulnerabilities	✓	✓	✓	✓
Launch Real Exploits & Denial of Service	✓	✓	✓	✓
Allowed to Change IP Addresses	✓	✓	✓	✓
Distributed Security Auditing	✓	✓	✓	✓
Automatic database and software updates	Yes	Yes	Yes	Yes

## Features

### Security Audit Features

- ✓ Vulnerability assessment
- ✓ 60.000 + vulnerabilities
- ✓ Unlimited auditing
- ✓ No software installation
- ✓ Advanced audit options
- ✓ Launch real exploits
- ✓ Security audit any OS
- ✓ Automatic web crawl script
- ✓ OS independent interface
- ✓ SANS top 20
- ✓ Malware Detection

### Easy-to-understand Reporting

- ✓ XML PDF and HTML reports
- ✓ Reports branding allowed
- ✓ Option for syslog remote logging

### Distribution Security Auditing

- ✓ Security audit remote locations from a centralized point
- ✓ Centralized reporting
- ✓ Centralized data storage
- ✓ Centralized control

### Security Audit Configuration

- ✓ Virtual host auditing
- ✓ Audit specific ports
- ✓ Audit specific web directories
- ✓ Email notification when an audit is finished

### Finds Cross Site Scripting, SQL Injection and Web Errors

- ✓ Automatic web crawling engine identifies known and unknown files on websites
- ✓ Finds Cross Site Scripting
- ✓ Finds SQL Injection
- ✓ Finds Web Errors
- ✓ Black Hat SEO Scanner
- ✓ Google Hack DB

### Multi User Support

- ✓ Supports multiple users to login at the same time
- ✓ Individual user accounts with different audit options and IP ranges
- ✓ Individual user security level
- ✓ Admin and regular users

### Scheduled Auditing

- ✓ Automatic scheduled auditing
- ✓ Automatic alert about new identified security vulnerabilities
- ✓ Shows new vulnerabilities discovered and compares them with old records to show the progress in the security level

### Scalable and Upgradeable

- ✓ All units can be upgraded for network growth via a software license
- ✓ Investment protection

### Penetration Testing

- ✓ Launch real exploits for Windows, Unix, Routers, Firewalls and more
- ✓ Launch real denial of service attacks
- ✓ Launch distributed denial of service via distributed setup

### Automatic Update

- ✓ Automatic daily database updates
- ✓ Automatic firmware updates with new features and functionality
- ✓ Centralized update point
- ✓ Automatic alerts when database is expired
- ✓ Option to upload updates manually via the interface

### Support & Maintenance

- ✓ One year database subscription included
- ✓ Full support included in price
- ✓ Option for instant replacement hardware
- ✓ Web-based user interface (https)
- ✓ Quick setup wizard
- ✓ Configuration backup/restore
- ✓ Email alert and logging via syslog
- ✓ Build-in diagnostic function

### Security Scanning of:

- ✓ Wordpress, Drupal, Magento, Shopify, Umbraco, Joomla, Webshops

E-mail: [info@secpoint.com](mailto:info@secpoint.com)



For more information on Penetrator, please visit  
<https://www.SecPoint.com/penetrator.html>  
<https://www.SecPoint.tv>

Partner Information