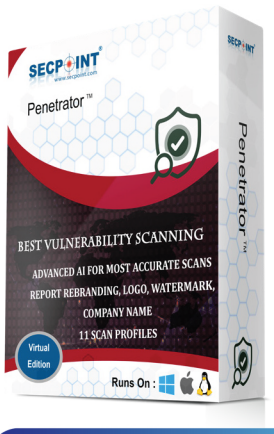
SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment



Windows Hyper-V

ESXi

itsecurity

PROTECTSTAR AWARD 2012

CVE COMPATIBLE cve.mitre.org

HIPAA COMPLIANT

SECPOINT®
www.secpoint.com

- √ 108,000+ Vulnerabilities
- √ 1,000+ Web Shells
- √ Cloud, Virtual Software 1U Appliance & SFF
- √ WiFi Pen Testing
- √ 19 Scanning Profiles
- √ Lethal Attack Technology SQLi, Blind SQLi
- √ Reflected XSS
- √ Distributed Node Scan
- √ Remote Code Execution
- √ Data Leak Detection
- √ TLS & SSL Vulnerabilities
- √ Scan IoT Devices
- √ Scan SCADA Systems
- √ 2FA Authentication
- √ AI Machine Learning
- √ Professional PDF & HTML
- √ Detailed Remedies
- √ SecPoint® RBL List
- √ Mitre CVE / Ubuntu USN / Microsoft / OSVDB
- √ Scan any OS or Network
- √ Reports Branding

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.

108,000 + Vulnerabilities

The Penetrator™ vulnerability database consists of continued research & development since 1998.
The database has a total of more than 108,000 unique remote vulnerabilities to scan for. The 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 scan different locations from a master Penetrator located in another city.

Vulnerability Scanning of any Operating System or Network Device

The Penetrator™ is designed to scan any operating system or network device. It is beneficial to scan 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 scan or resold as (SAAS) to your own customers.

SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment

Specifications	SecPoint® Penetrator™ S9 - 4-32 IPs	SecPoint® Penetrator™ S9 - 8-64 IPs	SecPoint® Penetrator™ S9 - 128-256 IPs	SecPoint® Penetrator™ S9 - 512-2048 IPs
Height	Small Form Factor (SFF)	1U Rackmount	1U Rackmount	1U Rackmount
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 AC/DC 100-240V	250w AC/ DC 100-240V	250w AC/ DC 100-240V	250w AC/ DC 100-240V
Environment Temperatures	Operating -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C
64 Bit Platform	√	√	√	√
SSD Included	√	√	√	√
Network Ports	4x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit
108.000 + Vulnerabilities	√	√	√	√
Launch Real Exploits & Denial of Service	√	√	√	√
Allowed to Change IP Addresses	√	√	√	√
Distributed Vulnerability Scanning	√	√	√	√
Automatic database and software updates	√	√	√	√

Features

Vulnerability Scan Features

- √ Vulnerability assessment
- √ 108,000+ Vulnerabilities
- √ 1,100+ Web Shells Detection
- √ Concurrent IP Scanning License
- √ Find missing Security Headers
- √ Advanced scan options
- √ File Upload Checks
- √ Vulnerability scan any OS
- √ Automatic web crawl script
- √ OS independent interface
- √ SANS top 20
- √ Malware Detection
- √ Lethal Attack - SQLi - Blind SQLi
- √ Data Leak Detection

Professional Reporting

- √ XML PDF and HTML reports
- √ Reports branding allowed
- √ Option for syslog remote logging
- √ 17 Report Languages

Distribution Vulnerability Scanning

- √ Node Vulnerability Scanning
- √ Centralized reporting, data storage, control

WiFi Auditing

- √ Audit WEP networks
- √ Audit WPA and WPA2 networks
- √ Test the security of your WiFi networks
- √ Identify hidden networks
- √ 2.4 GHz & 5 GHz
- √ 8 dBi Antenna
- √ Professional PDF Report
- √ Report Logo, Name & Watermark Branding

Vulnerability Scan Configuration

- √ Virtual host scanning
- √ Scan specific ports
- √ Scan specific web directories
- √ Email notification when an scan is finished
- √ 2FA Google Authenticator Support

XSS - SQLi - Blind SQLi & Web Errors

- √ Automatic web crawling engine identifies known and unknown files on websites
- √ Cross Site Scripting (XSS) & Reflected XSS
- √ SQL Injection & Blind SQL Injection
- √ Finds Web Errors
- √ Remote Code Execution (RCE)
- √ Advanced AI, Machine Learning
- √ Extensive TLS & SSL checks

Multi User Support

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

Scheduled Scanning

- √ Automatic scheduled scanning
- √ 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

Firewall

- √ On board Firewall
- √ SecPoint® RBL List
- √ Blocks 640+ Million Toxic IPs

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
- √ Full Data Privacy Menu

Security Scanning of

- √ CMS Vulnerabilities
- √ Wordpress, Drupal, Magento, Shopify, Umraco, Joomla, Webshops, SCADA, IoT

SECPOINT®
www.secpoint.com

For more information on SecPoint® Penetrator™, please visit
https://www.SecPoint.com/penetrator.html

Copyright © 1998-2022 SecPoint® www.SecPoint.com All rights reserved

VAR/VAD Contact

OFFICIAL PHILIPPINE DISTRIBUTOR
IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY
1004 Antel Global Corporate Center, #3
Julia Vargas Ave. Ortigas Center,
Pasig City, Philippines
Phone: +63 (2) 8638 - 3264
Email: inquiry@ipsystems.ph
Website: www.ipsystems.ph