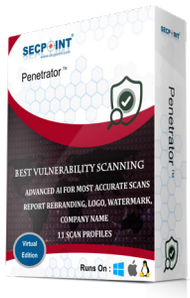
SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment



Windows Hyper-V™

ESXi

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

CYBERSECURITY MADE IN EUROPE

European DIGITAL SME Alliance — Issued by the European DIGITAL SME Alliance

itsecurity

ProtectStar AWARD 2012

CVE COMPATIBLE cve.mitre.org

HIPAA COMPLIANT

SECPOINT®
www.secpoint.com

- √ Powered by 141,000+ Vuln db
- √ 1,400+ Web Shells Detected
- √ Cloud & Virtual Software 1U Appliance & SFF
- √ WiFi Penetration Testing
- √ Node Scanning Capability
- √ Dark Web Search 4.0
- √ 31 Scanning Profiles Available
- √ 23 Report Languages
- √ Lethal Attack Technology SQLi, Blind SQLi & RCE
- √ Reflected XSS Detection
- √ Authenticated Scan Cisco & Linux
- √ Data Leak Detection
- √ TLS & SSL Vulnerabilities
- √ IoT Devices Scanning
- √ SCADA System Scanning
- √ Multi Factor Authentication
- √ AI Machine Learning
- √ Professional Reports PDF & HTML
- √ Detailed Remediation
- √ Mitre CVE / Ubuntu USN / Microsoft Bulletins & OSVDB
- √ SecPoint® RBL List Integration
- √ White Labeling Available
- √ Managed Service Provider (MSP)
- √ Full Data Privacy Menu

PREVENT UNAUTHORIZED ACCESS TO YOUR SERVERS AND NETWORK

A vulnerability assessment is a cornerstone of any robust security strategy. With the advent of sophisticated automated hacking tools, threats can propagate across networks and around the world in mere hours. Recognizing and addressing the potential vulnerabilities in your system is essential for maintaining its security.

The SecPoint® Penetrator™: Comprehensive Network Security

The SecPoint® Penetrator™ is both a virtual software and a hardware rack appliance designed for vulnerability assessment and penetration testing of your network. Arriving pre-loaded, it's primed for immediate deployment right out of the box. With its potent capabilities, user-friendly interface, and smart security assessment features, The Penetrator™ stands as a leading solution in its class..

Powered by 141,000+ Vulnerability Signatures

The SecPoint® Penetrator™ boasts a comprehensive vulnerability database, a testament to continuous research and development efforts since 1997. Users are equipped with an extensive range of scans. To ensure relevance and accuracy, the database receives multiple updates daily.

White-label Report Branding

Customize reports with your own logo, watermark, and company text. The Penetrator™ allows for full branding and personalization, empowering you to sell these reports as a unique service offering.

Distributed Node Scanning

Leverage the power of node scanning across a distributed network. The Penetrator™ offers several key advantages, including:

- Centralized reporting for cohesive insights
- Unified vulnerability assessment across all nodes
- A singular update point for streamlined maintenance

Moreover, it grants the capability to scan various locations remotely, even if the master Penetrator is situated in a different city.

Universal Vulnerability Scanning

The Penetrator™ is equipped to scan any operating system or network device. It's crucial to assess every device within your network infrastructure, identifying and addressing vulnerabilities before they can be exploited by attackers.

Managed Service Provider (MSP)

All Penetrators support multi-user login. This could be used to create different accounts with different targets to scan, custom policy and 2fa enabled or resold as (SAAS) to your own customers.

With the Super Admin interface control users easily.

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 SFF with 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
Network Ports	4x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit
Lethal Attack - SQLi - Blind SQLi	√	√	√	√
Network Ports	√	√	√	√
Database of 133,000+ Vulnerabilities	√	√	√	√
Whitelabeling & MSP Support	√	√	√	√
Allowed to Change IP Addresses	√	√	√	√
Distributed Vulnerability Scanning	√	√	√	√
Automatic database and software updates	√	√	√	√

Features

Vulnerability Scan Features

- √ Vulnerability Scanning & Assessment
- √ Database of 141,000+ Vulnerabilities
- √ Database of 1,400+ Web Shells
- √ Dark Web Search 4.0
- √ Advanced scan options available
- √ Capability to launch Real Exploits
- √ File Upload Vulnerability Checks
- √ Compatible with scanning any OS
- √ OS independent interface
- √ SANS top 20 vulnerability checks
- √ Malware Detection capabilities
- √ Lethal attack detections (SQLi) & Blind SQLii
- √ Identification of missing security headers

Easy-to-understand Reporting

- √ XML PDF and HTML reports
- √ Whitelabeling Reports branding
- √ 23 Report Languages

Distribution Vulnerability Scanning

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

WiFi Penetration Testing

- √ Audit WEP, WPA & WPA2 networks
- √ Identify hidden networks
- √ Supports both 2.4 GHz & 5 GHz frequencies
- √ Supports 8 dBi Antenna
- √ Provides a professional PDF report

Vulnerability Scan Configuration

- √ Virtual host scanning
- √ Scan specific ports & web directories
- √ Email notification when an scan is finished
- √ Authenticated scanning for Cisco & Linux systems
- √ 31 Scanning Profiles Available

Detection of Web Vulnerabilities & Errors

- √ Automatic web crawling engine identifies both known & unknown files on websites
- √ Detects Cross Site Scripting(XSS)
- √ Identifies Reflected Cross Site Scripting
- √ Discovers SQL Injection vulnerabilities
- √ Locates Web Errors
- √ Comprehensive TLS & SSL checks
- √ Remote Code Execution(RCE)
- √ Scan Target Location via Geo Mapping

Multi User Support

- √ Supports concurrent user logins
- √ Individual user accounts with customizable scan and IP ranges
- √ Defined user security level
- √ Distinguishes between admin, regular users, and super admin
- √ Super Admin Interface available
- √ Suitable for Managed Service Providers (MSP)
- √ Multi Factor Authentication (MFA) supported for admin and individual users

Scheduled Vulnerability Scanning

- √ Supports automatic scheduled scanning
- √ Sends alerts for newly identified security vulnerabilities
- √ Displays new vulnerabilities, comparing them with previous records to highlight changes

Firewall

- √ On board Firewall
- √ SecPoint® RBL List
- √ Blocks Millions of Toxic IPs
- √ Blocks Entire Undesired Countries

Scalable and Upgradeable

- √ Units are upgradeable to accommodate network growth through a software license
- √ Ensures protection of your investment

Penetration Testing

- √ Launches real exploits for platforms including Windows, Unix, Routers, Firewalls, and more
- √ Executes real denial of service attacks
- √ Initiates distributed denial of service through a distributed setup

Automatic Update

- √ Provides automatic daily database updates
- √ Offers automatic firmware updates introducing new features and functionality
- √ Centralized update point available
- √ Sends automatic alerts when the database expires
- √ Includes an option for manual update uploads via the interface

Support & Maintenance

- √ Full support encompassed in the price
- √ Features a web-based user interface (https)
- √ Quick setup wizard for easy initialization
- √ Offers configuration backup & restore functionality
- √ Supports email alerts
- √ Build-in diagnostic function
- √ Full Data Privacy Menu
- √ Terminal Console Access
- √ Expert Cybersecurity Human Support not AI Robot

Security Scanning of

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

SECPOINT®
www.secpoint.com

For detailed information on the SecPoint® Penetrator™,
visit the official webpage at **https://www.SecPoint.com/penetrator.html**

Value Added Reseller(VAR) / Value Added Distributor(VAD)