SecPoint® Penetrator™

- 64 Bit High Performance
- Scans Local & Public IPs
- Best Vulnerability & Assessment Scanning
- Easy Solutions to found vulnerabiliites
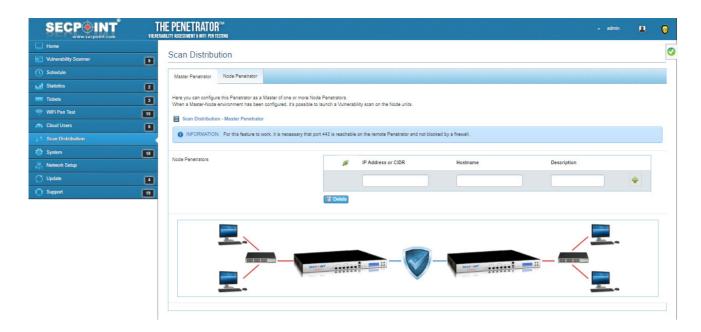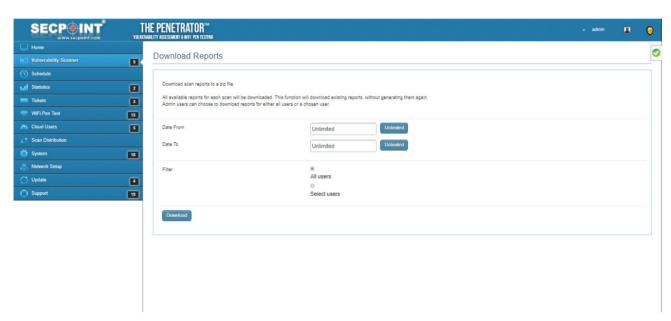- Virtual VMware & Hyper-V Support

Windows Hyper-V™

ESXi

The Penetrator™

SECPOINT®
www.secpoint.com

Best Vulnerability Scanning
Penetration Testing
Launch Real Exploits

Free Bonus DVD

vmware READY

Clear Solutions to
fix the found Vulnerabilities
50.000+ Checks
SEO Blackhat Scanner
Web Vulnerability Crawler
The Penetrator™

Runs on

HAKIN9
SECURING VOIP

ProtectStar
AWARD
2012

CVE COMPATIBLE
cve.mitre.org

SECPOINT®
www.secpoint.com

Advanced AI
Cyber Security

vmware® READY

Prevent Hackers from entering your server and network!
Vulnerability management 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 minutes. Understanding the potential vulnerabilities within your system is vital to any security strategy.

SECPOINT®
www.secpoint.com

Scan Distribution

Master Penetrator | Node Penetrator

Here you can configure this Penetrator as a Master of one or more Node Penetrators.
When a Master-Node environment has been configured, it's possible to launch a Vulnerability scan on the Node units.

Scan Distribution - Master Penetrator

ℹ INFORMATION: For this feature to work, it is necessary that port 443 is reachable on the remote Penetrator and not blocked by a firewall.

Node Penetrators

	IP Address or CIDR	Hostname	Description	
				✚

🗑 Delete

Download Reports

Download scan reports to a zip file.

All available reports for each scan will be downloaded. This function will download existing reports, without generating them again.
Admin users can choose to download reports for either all users or a chosen user.

Date From   Unlimited   [Unlimited]

Date To   Unlimited   [Unlimited]

Filter
- ◉ All users
- ○ Select users

[Download]

Vulnerability management
is key to any security strategy

Vulnerability Management

The Penetrator is a vulnerability management and penetration testing appliance for your network, which comes pre-loaded and ready to go.
It is a powerful and intelligent security assessment solution.

Comprehensive Vulnerability Scanning

With its comprehensive vulnerability database and the application of sophisticated auditing techniques, the Penetrator enables you to
always be one step ahead of even the most skilled and advanced attackers. It has no limit on the amount of auditing nor limit on the number of IP addresses and is most certainly one of the strongest and most comprehensive vulnerability assessment solutions on the market.

Professional Skilled Support

Second to none with the fastest reply and response rate to support queries in the industry.
The best 24 Hour skilled support team operation.
Fast remote login with problem solving via TeamViewer.
Follow Support Ticket Status via the Support Center.

SecPoint Penetrator™

Penetration Testing Appliance

Easy-to-understand Reporting

Reports can be customised and are available as XML, PDF or HTML files.

System vulnerabilities are categorised as either high risk, medium risk or low risk, together
with name and details of each vulnerability and its solution..
The report also gives a conclusion as to the overall security level of the audited system.

An executive summary is compiled specifically for
management level review with both text and graphical details from the audit results.

Easy to install

The Penetrator is compatible with any operating system. It is easy to install, with minimal configuration. Installation wizards provide for fast set up.

Scalable and Upgradeable

The Penetrator is scalable for network growth and IP addresses.

Distributed Audit Capability

You can setup multiple Penetrator at different
locations on the internal network and remotely via an encrypted secure connection connect them together. This allows distributed auditing, configuration and reporting from a centralized point.

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.

Features and Benefits

- No Data Collection, Backdoor Free

- 11 Scan Profiles, HIPAA,OWASP top 10, Prepare for PCI, Firewall Scan, SCADA and more

- Advanced Web Crawler - SQL Injection - XSS - SSL

- Bugtraq ID / Mitre CVE / Ubuntu USN / Microsoft / OSBDB

- Schedule scans daily,weekly,monthly

- Prevent Hackers To Access Your Server

- Vulnerability Scanning

- Vulnerability Assessment

- 60.000 + Vulnerabilities
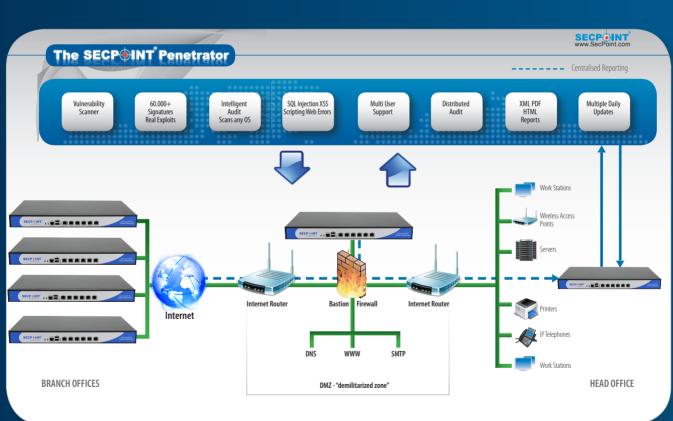
- Launch Real Exploits

- Distributed Scanning Capability

- Report languages: English, Spanish, Danish, Italian, Korean, Dutch, Norwegian, Thai, Portuguese, Turkish & Croatian

- Scan any OS and Network devices

- Reports Branding

- Detailed Remedies for Identified Vulnerabilities

- Secure Design All Data Stored on Unit

- Ticket System for full Vulnerability Management

- Vulnerability Audit

- Launch DoS & DDoS attacks

- Advanced Audit Options

- Option for centralized update point

- Audits any OS

- Automatic Web Crawl Script Engine

- Stand-Alone SFF or 1U Appliance

- Multi User Support

- Launch Real Exploits

- Option for syslog remote logging

- OS Independent Interface

- Distributed Auditing

- XML, PDF and HTML Reports

- Finds SQL Injection

SecPoint® Penetrator™
Penetration Testing Appliance

SecPoint® Penetrator™ Models >>

	S9 - 4-32 IPs	S9 - 8-64 IPs	S9 - 128-256 IPs	S9 - 512-2048 IPs
Height	1 U Rackmount Small Form Factor SFF	1U Rack mount	1U Rack mount	1U Rack mount
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
Network 10/100/1000 Mbpsh	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces
Automatic database and software updates	Yes	Yes	Yes	Yes

Are you ready for the next step?

The SECP✣INT Penetrator
www.SecPoint.com

Centralised Reporting

| Vulnerability Scanner | 60.000+ Signatures Real Exploits | Intelligent Audit Scans any OS | SQL Injection XSS Scripting Web Errors | Multi User Support | Distributed Audit | XML PDF HTML Reports | Multiple Daily Updates |

Work Stations
Wireless Access Points
Servers
Internet
Internet Router
Bastion Firewall
Internet Router
Printers
IP Telephones
Work Stations
DNS   WWW   SMTP
BRANCH OFFICES
DMZ - "demilitarized zone"
HEAD OFFICE

E-mail: info@secpoint.com

SECP✣INT®
www.secpoint.com

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

Partner Information