



Service Overview

PCI Scanning Services

March 2008

All SensePost documentation contains confidential and proprietary information. Any information contained in such documents may not be made available to any third party without the written authorization of an authorized SensePost representative.

Document Information

A document for: **SensePost**
Document description: **PCI Scanning Services**
Document completion date: **2008-03-19**
Document number: **PCI_ASV_20080319**
Issue: **1.0 (Final)**
Last modified: **2008-03-21**
Author: **Nicholas Arvanitis**

SensePost Contact Details

Physical Address	Postal Address	Contact Number	Fax Number
Lakeview II 138 Middel Street Nieuw Muckleneuk Pretoria South Africa	P.O Box 176 Groenkloof 0027 South Africa	+27 12 460-0880	+27 12 460-0885

Contact E-Mail Addresses

General: info@sensepost.com www.sensepost.com
Training: training@sensepost.com
Research: research@sensepost.com
PCI Services: pci@sensepost.com

Revision History

Document Version	Description	Date	Author
0.1	First Draft	2008-03-18	Nicholas Arvanitis
0.2	Peer Review	2008-03-20	Charl van der Walt
0.5	Commercial QA		
1.0	Final		Nicholas Arvanitis

All SensePost documentation contains confidential and proprietary information. Any information contained in such documents may not be made available to any third party without the written authorization of an authorized SensePost representative.



Table of Contents

1	Introduction	4
1.1	Service Overview	4
1.2	SensePost Capabilities Summary	4
1.3	Deliverables.....	4
2	The HackRack PCI Security Scanner	6
3	Scoping and Pricing Breakdown	10

Tables

Table 1 - Scoping and Pricing Breakdown.....	10
--	----

Figures

Figure 1 - Configuration Interface - Scan Scheduling.....	7
Figure 2 - Interactive Scan Result Interface.....	8
Figure 3 - PDF Report Excerpt.....	9



1 Introduction

This document presents an overview of the SensePost *PCI Approved Scanning Vendor (ASV)*-based network scanning services, which are aimed at producing the required reports for the purposes of compliance with the *PCI Data Security Standard (DSS)*. A pricing breakdown is also included, to explain the different bands of pricing for the service.

1.1 Service Overview

In this document, SensePost proposes to assist organizations by conducting the network-based vulnerability scanning and producing the relevant reports required for submission to the relevant acquiring bank in order to fulfil that portion of the obligation to the *PCI DSS*.

More information on the *PCI*-specific terms and requirements relative to organizations and this document are provided in **Section 7 – PCI Glossary and Requirements Overview**.

A brief summary of the services that are proposed is included below:

Description	Summary	Validation	Duration
<i>HackRack PCI Scanning</i>	<i>Unlimited network scanning and reporting performed by an accredited ASV, to fulfil the quarterly scan obligation imposed by the PCI DSS.</i>	<i>Compulsory</i>	<i>Annual</i>

1.2 SensePost Capabilities Summary

SensePost is already well established as an independent and leading Information Security services provider in both the South African and International markets. SensePost plays the role of a trusted advisor to wide variety of clients when it comes to Information Security, is recognized as a global thought leader in the field, and offers a broad range of services to the market.

HackRack – SensePost’s automated vulnerability scanning service – has been developed over the last seven years to scan and monitor an organization’s *Internet facing* infrastructure. The purpose of *HackRack* is to perform continuous, repetitive vulnerability scans against all Internet-facing systems in order to immediately detect new threats that arise when client configurations change or when new vulnerabilities are discovered.

Both SensePost as a company and the *HackRack* technology have completed the *PCI* relevant *PCI DSS* accreditation processes and are formally accredited by the *PCI SSC* as an ASV with certificate number 4239-01-01.

More information on SensePost, its skills and its technologies is available on request.

1.3 Deliverables

The SensePost *HackRack PCI* scanning service model is fairly simple in concept - the customer receives an account on SensePost’s *HackRack PCI* system and can use it to configure and run scans as often as is required.

Although the requirement in terms of the *PCI DSS* is to run quarterly scans, the customer is in no way limited to this, and is able to run scans as and when they please.

PCI Compliance scanning includes everything needed to make the process simple and easy, including:

- Unlimited access to our web-based interface
- Scan scheduling

SensePost PCI Services
PCI Scanning Services



Document Number:

PCI_ASV_20080319

Date:

2008-10-03

- Unlimited on-demand manual scans
- Issuing a *Certification of Compliance* accepted by all credit card companies and all banks worldwide
- Support and maintenance allowing access to skilled SensePost analysts to verify and clarify reported issues



2 The HackRack PCI Security Scanner

Over the last seven years SensePost has developed a unique approach to security assessments that combines aggressive, detailed analysis with continuous, repetitive vulnerability scans. This approach has numerous advantages, not least of which is the detection of new threats that arise when client configurations change or when new vulnerabilities are discovered. The continuous daily scans are performed using *HackRack* – SensePost’s automated vulnerability scanning service.

HackRack is an automated security scanner developed by SensePost that monitors an organization’s *Internet-facing* infrastructure. The purpose of *HackRack* is to perform continuous, repetitive vulnerability scans against all Internet-facing systems in order to immediately detect new threats that arise when client configurations change or when new vulnerabilities are discovered.

Full vulnerability reports are generated on a regular basis, detailing all the issues found on the target systems, as well as information on how the problem can be verified and what remediation action is required. Furthermore, reports are generated on a daily basis describing only *new* issues that were discovered from that day’s scans.

Graphical management reports depict valuable summary information, including a risk-impact breakdown of all issues discovered, the most serious hosts, the most serious problems and various trends and statistics. The web-based graphical reports are fully interactive and allow users to drill down into the system, obtaining more detailed information or requesting new or different tests.

Notification of new reports is delivered at the same time daily to the relevant administrators via secure email. Notifications can be sent to a central security-management team as well as any number of predefined system owners.

On receipt of the notification the administrator can access the system via the URL provided and view or manage only those reports relevant to his or her particular section. All functional areas of the report remain accessible.

The *HackRack PCI* service runs from a set of servers located on the Internet and is fully managed and maintained by SensePost. There are no setup, configuration or infrastructure costs. The service can be started or paused at any time, but proceeds in a fully automated fashion.

The *HackRack PCI* service is fully supported by SensePost. Customers have access to a graphical web interface via which they can view reports, graphs and statistics, change basic configurations, initiate new scans and log tickets. In addition, *HackRack* scans can be launched at any time against any legally authorised host.

All levels of support are offered directly by SensePost. Support can be requested directly from the vulnerability report via the web interface. The level and quality of support offered by SensePost is key to this service and is what differentiates this offering from any other of its kind on the market.

The *HackRack* technology is fully owned, developed and supported by SensePost. It has been in production since 2001. The *HackRack PCI* technology was developed in 2007 in order to extend *HackRack*’s capabilities and allow *HackRack* to be used as a platform for the quarterly network scans and specific requirements of the *PCI DSS*. *HackRack PCI* and SensePost are fully accredited as a *PCI ASV* with certificate number 4239-01-01.

Some sample images from the solution are provided in subsequent pages, below.



The first image, depicts the configuration interface, in this case, specifically for scheduling of the scans.

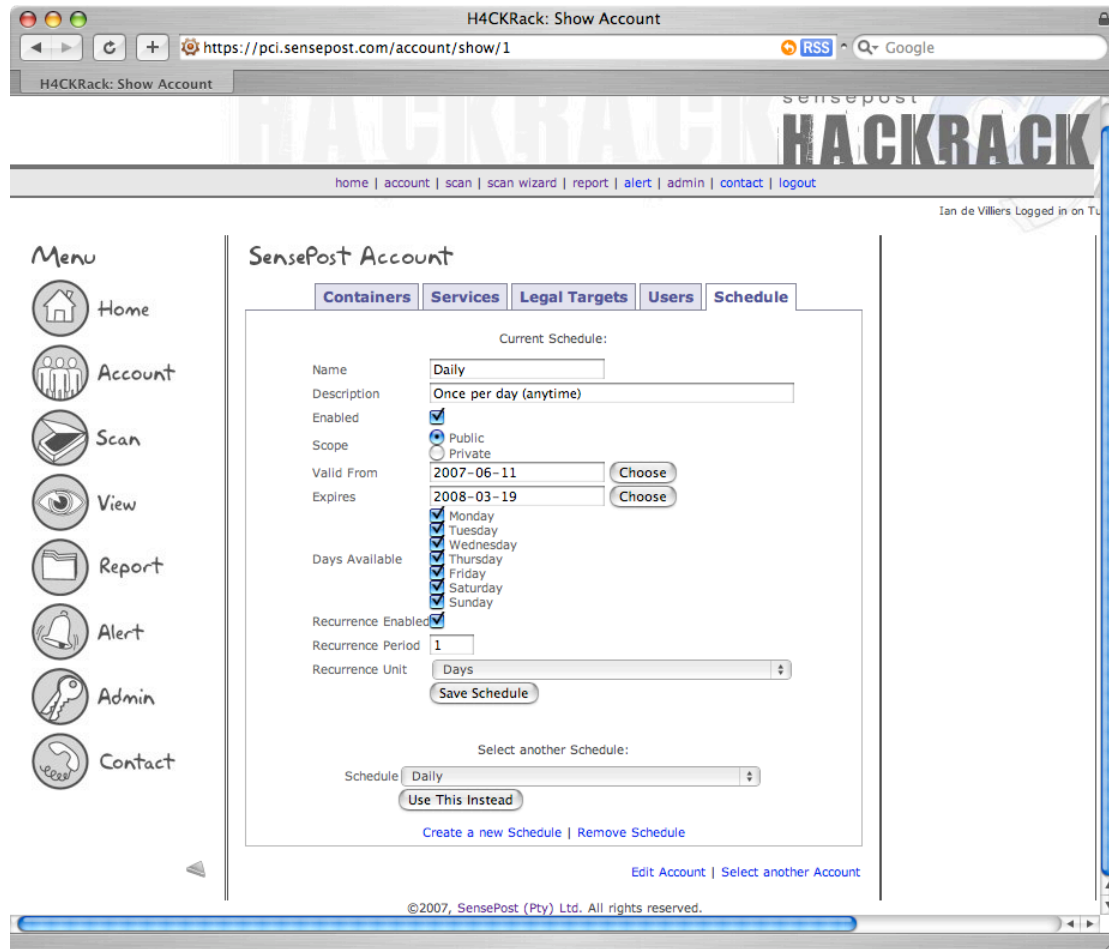


Figure 1 - Configuration Interface - Scan Scheduling

The image which follows shows the interactive web-based interface for examining scan results – a simple example is presented in the image provided.

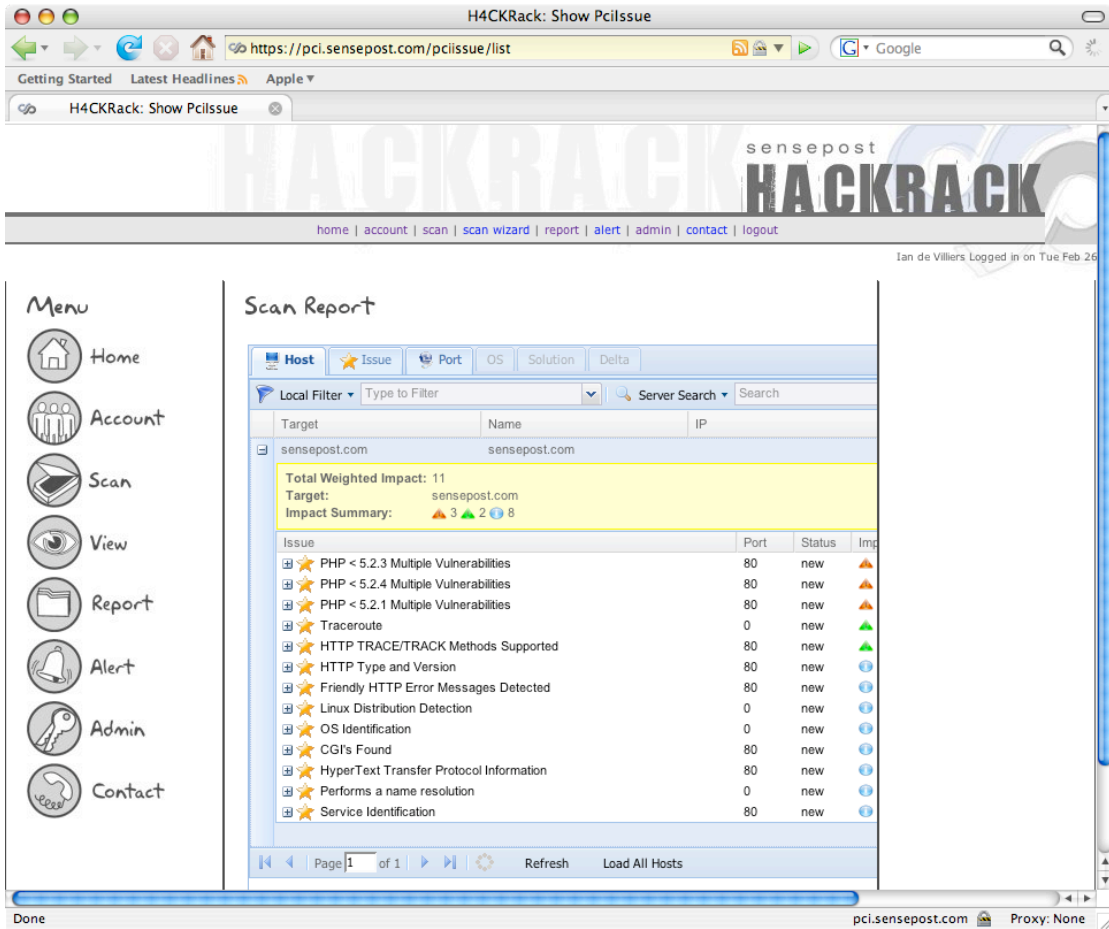


Figure 2 - Interactive Scan Result Interface

Finally, the solution allows reports to be exported in PDF format, and downloaded. The image below is an example of an excerpt from such a report.

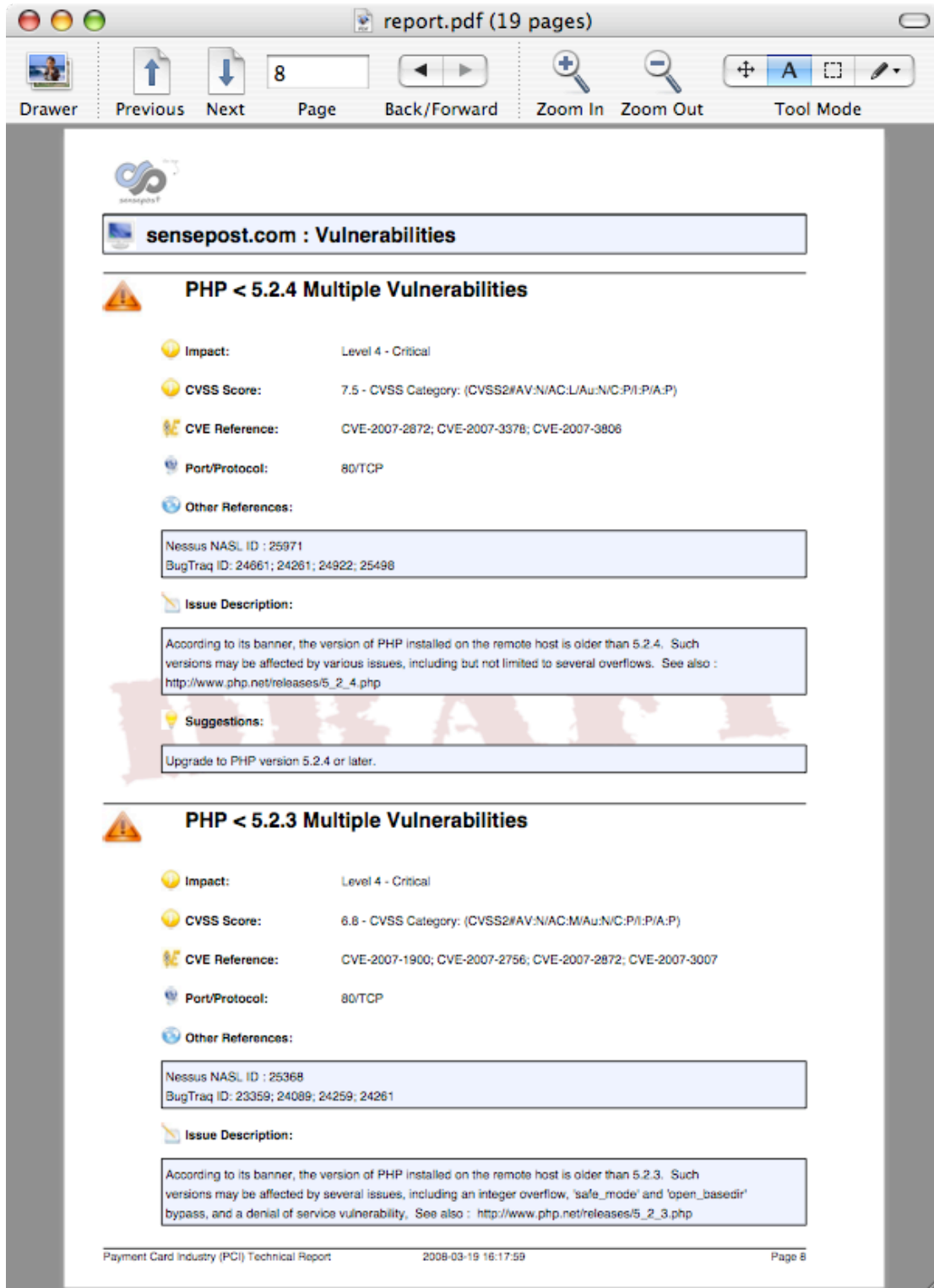


Figure 3 - PDF Report Excerpt



3 Scoping and Pricing Breakdown

3.1 Scanning

The pricing model for SensePost's *HackRack PCI* service is provided in the table below:

Service Scale	Annual Costing (USD\$ Per IP)
PCI Scanning of 1-5 IP Addresses (Per IP per Year)	144.00
PCI Scanning of 6-20 IP Addresses (Per IP per Year)	120.00
PCI Scanning of 21-50 IP Addresses (Per IP per Year)	108.00
PCI Scanning of over 50 IP Addresses (Per IP per Year)	84.00

Table 1 - Scoping and Pricing Breakdown

3.2 Support

SensePost offers a comprehensive support service around the vulnerability scanner that ensures the customer fully understands the findings in the report and the implications of those findings within the context of the report. Thus, in addition to the automated scans that the customer may request at any time, SensePost will manually oversee the execution each required quarterly scan and oversee the findings in the report to verify their accuracy and relevancy with regard to the DSS. Moreover, experienced SensePost analysts are available on a business-hours basis throughout the year to field any queries and provide support around scanner output.

Service Scale	Annual Costing (USD\$)
Annual support plus quarterly scan management and executive oversight of quarterly scans	5,500.00