



JANUARY 2010

SENSEPOST

SensePost was founded in 2000 by internationally recognised industry experts and has become one of the foremost Information Security consultancies in the world market.

THE VISION

Our vision is to use premier people, leading-edge technology and progressive thinking to provide Information Security services that add value to business.

SERVICES

- Technical Information Security Assessments
- Information Security Consulting
- Vulnerability Management Services
- High end Information Security Training

DIFFERENTIATORS

SensePost has built a global reputation based on world-class skills, a demonstrable track record in vulnerability research and a blue-chip client list.

T: +27 12 460 0880
F: +27 12 460 0885
E: info@sensepost.com

www.sensepost.com

PO Box 176
Groenkloof
0027
South Africa
Reg No 1999/004700/07

WHY ASSESSMENTS?

Effectively securing an organization's information assets must at some stage entail active testing of the security measures deployed, in order to practically validate assumptions about the efficacy of these solutions.

Such testing is mostly successful in enumerating oversights and flaws in security architectures precisely because it discounts the 'protective' mindset and bends the 'rules' envisaged by security professionals, by adopting an adversarial approach.

Ultimately, attackers don't think like security professionals – thus, in order to appropriately

measure the risks posed by compromise attempts, empirical evidence of the impact of attacks targeting information assets must be analyzed from the perspective of a skilled and motivated attacker.

Security assessment services aim to provide insight into the impact of these risks by simulating targeted attacks against the organization.

QUICK FACTS

What: A controlled attack against an application or infrastructure with value to your business.

Why: To practically verify the security posture of the system and provide assurance that it is resistant to attack.

How: Various approaches cater to differing needs and budgets at all layers of a system's stack, with the main distinction being between 'once-off' and 'continuous' assessments.

Who: SensePost analysts are experienced technical specialists with extensive skill sets and a proven record in the international arena.

APPROACHES

Security Assessments and Penetration Testing are often used interchangeably to describe the same thing and as a result the value and deliverables of each are confused. Whilst each of these spheres is indeed complimentary, and at times overlapping, each class of service does provide fairly distinct deliverables.

A brief overview of each of these service spheres is outlined below, to attempt to differentiate these services.

Penetration Testing:

A Penetration Test is essentially an attempt by an ethical hacker, working under strict constraints to compromise a specific system, set of systems or data.

Such an exercise is generally quite effective in answering the question 'can we be compromised'? However, it does not provide a complete view of what and where all the exploitable weaknesses are.

Security Assessments:

A Security Assessment usually includes some degree of Penetration Testing, but it takes a more formal and systematic approach and provides a comprehensive view of where all the exploitable vulnerabilities are and what should be done to remediate them.

This makes the Security Assessment a very valuable exercise for decision makers. An Assessment presents a point-in-time view of the target security posture. Of course, this view can change rapidly as new attack vectors are developed, as the target itself changes or even as the issues are remediated.

ASSESSMENT SERVICE DEFINITIONS

Essentially, an organization needs to assess its security posture from 3 perspectives, briefly outlined below:

APPLICATION LAYER

The number of web applications, which expose business logic both internally and externally is increasingly defining an organization's footprint. This exposed and distilled business logic makes such applications a prime target for attack.

Such applications are either purchased off the shelf or are custom developed. Application security is major shortcoming across the board, and compromises of custom as well as vendor-developed applications seem to escalate on a daily basis. Due to the nature and/or strategic placement of these applications it is critical for an organization to assess their security posture.

SensePost offer application assessments on both rich client and browser-based applications.

INTERNET INFRASTRUCTURE

This perspective entails the resources and services an organization has exposed to the public Internet.

Most, if not all organizations today require some form of connectivity to various external providers, business partners and similar, and consequently must expose certain resources publicly. This is even more apparent for organizations that conduct commerce using the Internet as a medium.

These services are accessible to most people surfing the Internet and thus by their nature exposed, therefore it is essential that this environment be regularly assessed to ensure that the security posture is of an acceptable standard.

INTERNAL INFRASTRUCTURE

In our experience, we have found that most organizations perceive the attacker threat to originate from an external location, which is largely unknown to the organization.

This assumption is the base from which an organization designs its security, which concentrates on services that are exposed to the Internet. Not much emphasis is given to the internal network, which is mostly left unsecured. At the same time, the composition of the organizational work force is changing - more

temporary or contract staff is employed. These "untrusted" employees have an elevated level of privilege on the network, which potentially makes them a threat to the organizational security.

It is no longer acceptable to allow the internal network to be left insecure. An organization needs to assess the internal network to identify vulnerabilities and threats which an employee can intentionally or unintentionally exploit, resulting in a compromise.

ASSESSMENT APPROACHES

In order to assist organizations to identify, manage and mitigate information security vulnerabilities and threats, SensePost have 3 primary approaches to assessments. These are listed below.

SPOT-CHECK

This is a once-off, short engagement, designed to quickly give an organization a snapshot of their security posture. Normally this type of assessment is a pre-cursor to a full-blown assessment.

BLACK-BOX

This approach is taken to demonstrate the vulnerability status of an organization as seen through the eyes of an anonymous attacker. Minimal prior knowledge of the target is given to the security analyst and the objective is to find and exploit as many vulnerabilities as possible.

The downside to this approach is that the analyst is governed by the time available for the project. This is not a restriction placed on a real life attacker.

In order to negate this restriction SensePost recommend a 'grey-box' approach, which requires an organization to be an active participator in the assessment process. A fair amount of prior knowledge is required to assist the analyst in getting to the real security issues rather than spending the majority of his time doing organizational reconnaissance.

HIGH ASSURANCE

As the name suggests this assessment attempts to give the organization the highest level of security assurance for the environment or application assessed.

This approach is typically used for mission critical applications and comprises of a black/grey box approach together with a source code review, or review of system architecture and policy configurations.

ASSESSMENT SERVICES OVERVIEW

The table below summarises an outline of the assessment services that SensePost can offer to assist organizations in assessing the security of their environments.

	INTERNET INFRASTRUCTURE	APPLICATION LAYER	INTERNAL INFRASTRUCTURE
SPOT CHECK	Our 'AVA' service constitutes a simple, automated scan against the target infrastructure to identify basic vulnerabilities and configuration issues.	Our 'AVA-Web' service constitutes a simple, automated scan against the target application to identify basic programming issues and configuration issues.	Our 'BAVA' service constitutes a simple, automated scan against the target infrastructure conducted from behind the corporate firewall.
BLACK-BOX ASSESSMENT	An Internet Security Assessment takes a formal and systematic approach and provides a comprehensive view of where all the exploitable vulnerabilities are and what should be done to remediate them.	SensePost employs in-house tools and methodologies to conduct web application assessments. The major part of a web assessment is conducted manually and is therefore a very resource intensive process.	An Internal Vulnerability Assessment looks at core LAN infrastructure from a basic security configuration perspective. This will identify misconfigurations, missing patches and other security vulnerabilities that could lead to a security compromise.
HIGH-ASSURANCE ASSESSMENT	A High-Assurance assessment includes a grey-box review of the Internet architecture and firewall rule-set.	A High-Assurance Application Assessment includes a Threat Model and grey-box targeted code review.	A High Assurance Assessment will also consider whether the security installation and configuration is considered according to security best practice, including Personal Firewalls, Antivirus, Updates, Software and patch versions, Security configuration and settings, Security management, User security behaviour, etc.
CONTINUOUS ASSESSMENT	Our 'HackRack' automated scanning service continuously scans the target infrastructure to detect new issues or changes that have introduced security weaknesses.	The HackRack 'Web Application Module' can scan the range of weaknesses as highlighted by the 24 WASC vulnerability classes such as Cross-Site Scripting, Directory Traversal, and SQL Injection.	'BroadView' is a fully managed service that uses SensePost proprietary technology and analyst expertise to systematically identify and manage host security vulnerabilities across the entire enterprise network.

