

SOPHIACONF 2015

SCAN DE VULNERABILITE AVEC OPENVAS

Frédéric Donnat – Directeur Technique

Fred@SecludIT.com

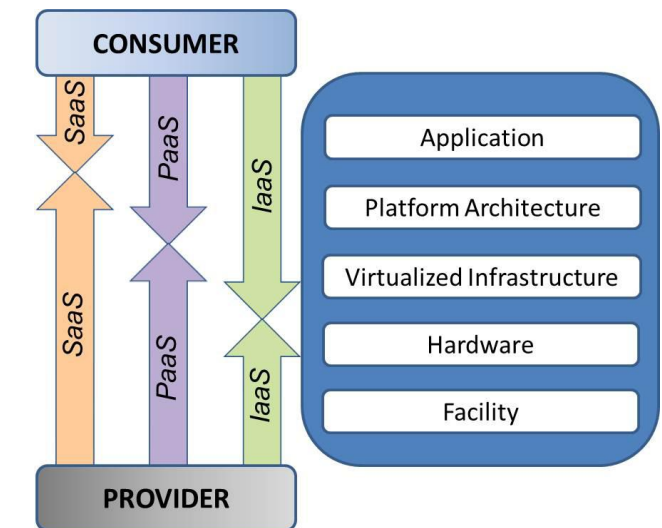
<http://secludit.com>

Juillet 2015

AGENDA

Cloud et modèle de « Partage de Responsabilité »

- 3 niveaux: IaaS, PaaS, SaaS



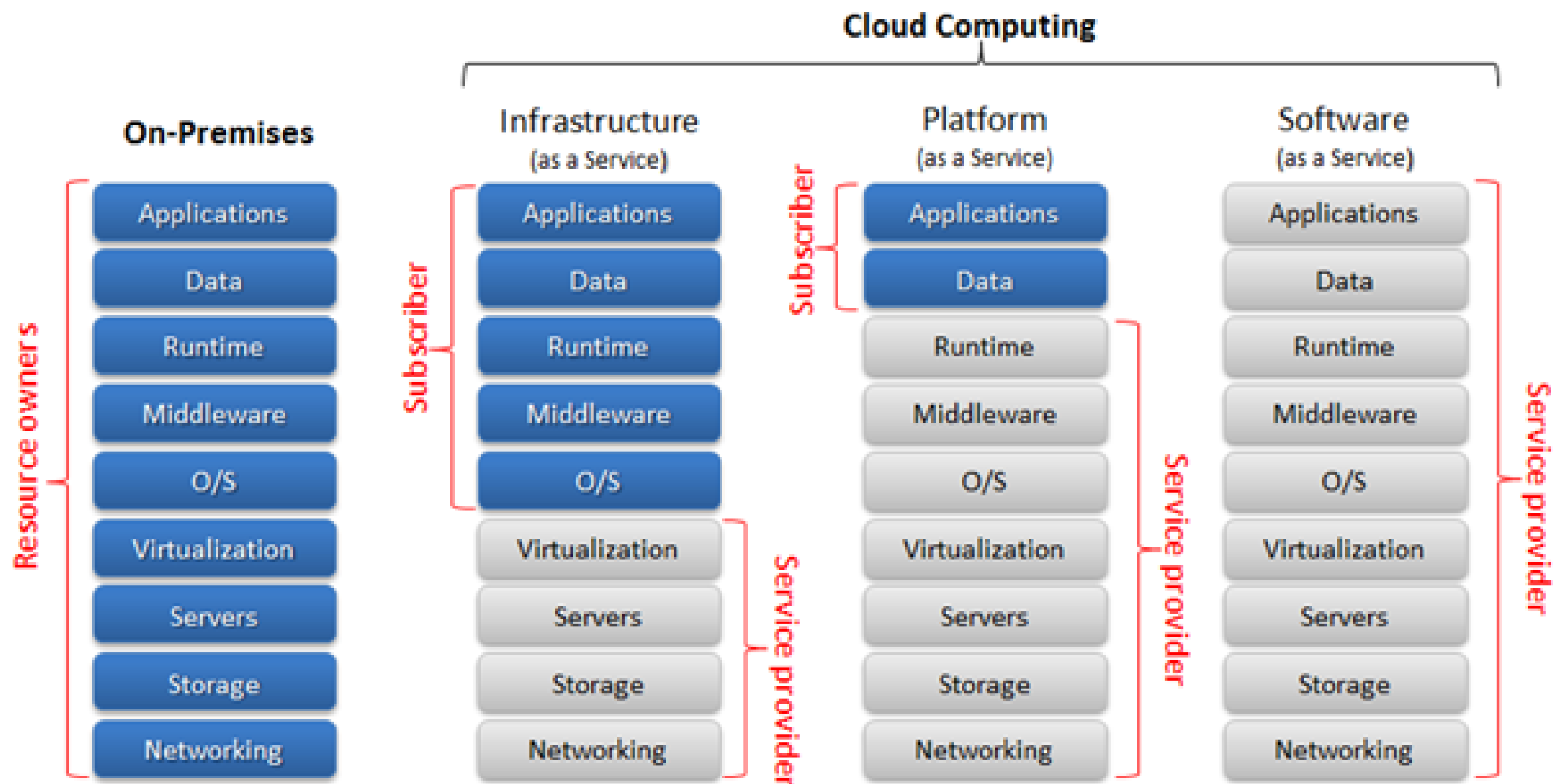
Cercle Vertueux

- Scan de Vulnérabilité, Test d'intrusion, Mise à jour, Remédiation


Cas d'étude : Scan avec OpenVAS



Separation of Responsibilities







Greenbone
Security Assistant

Logged in as Admin admin | Logout
Thu Jul 2 19:51:10 2015 UTC

Scan Management

Asset Management

SecInfo Management

Configuration

Extras

Administration

Help

Tasks 1 - 2 of 2 (total: 2)

Filter: apply_overrides=0 rows=10 first=1 sort=name

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
OWASPBWA - Creds Scan	Done	1		Jul 2 2015	High		
OWASPBWA - NoCreds Scan	Done	1		Jul 2 2015	High		


(Applied filter: apply_overrides=0 rows=10 first=1 sort=name)

Welcome dear new user!

To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon



Quick start: Immediately scan an IP address

IP address or hostname:

Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List

2. Create a new Task using this target with default Scan Configuration

3. Start this scan task right away

4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the details icon and review the results collected so far.

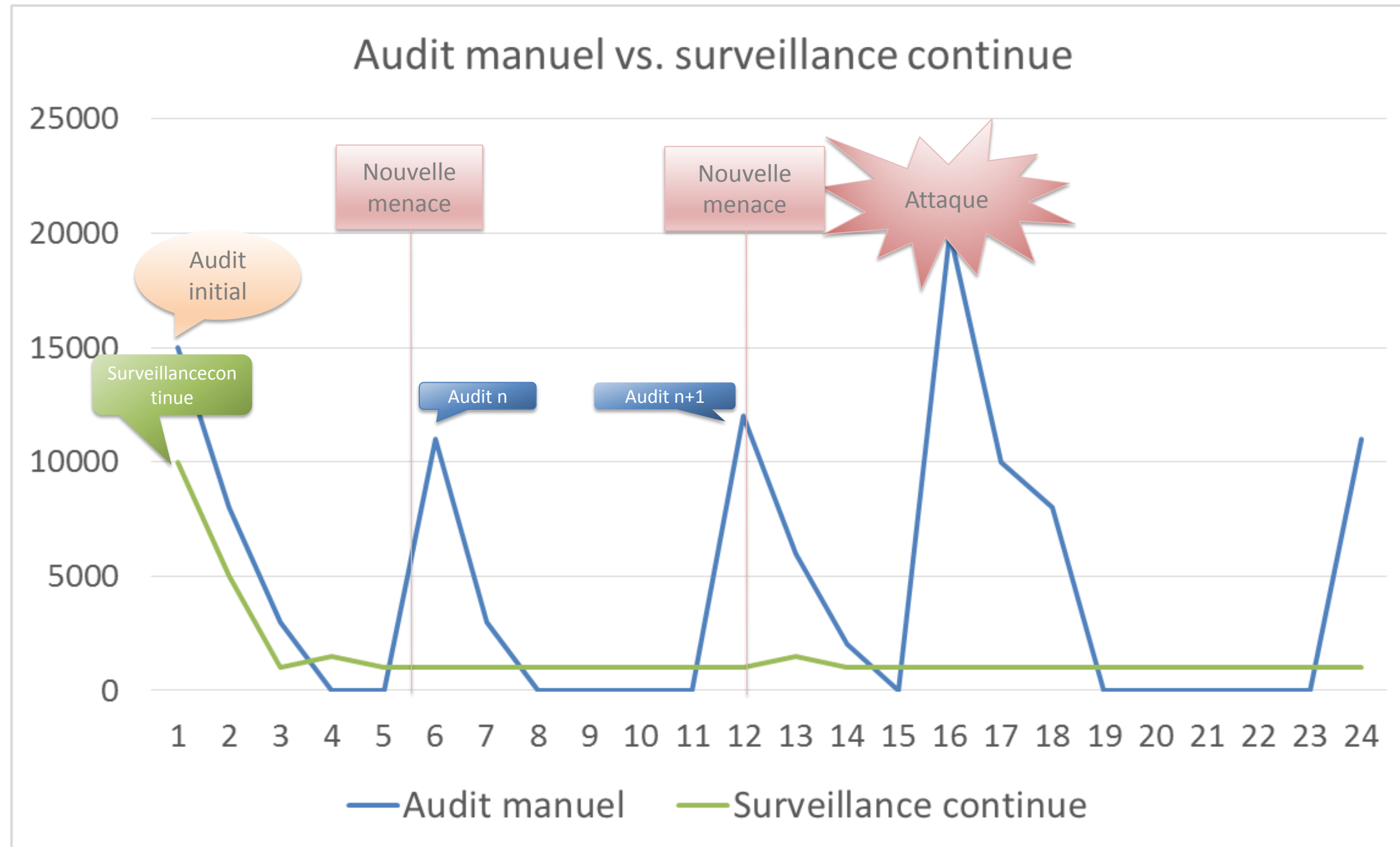
```
graph TD; A[Scan de Vulnérabilité] --> B[Test d'Intrusion]; B --> C[Mise à jour]; C --> D[Remédiation]; D --> A;
```

SECLUD

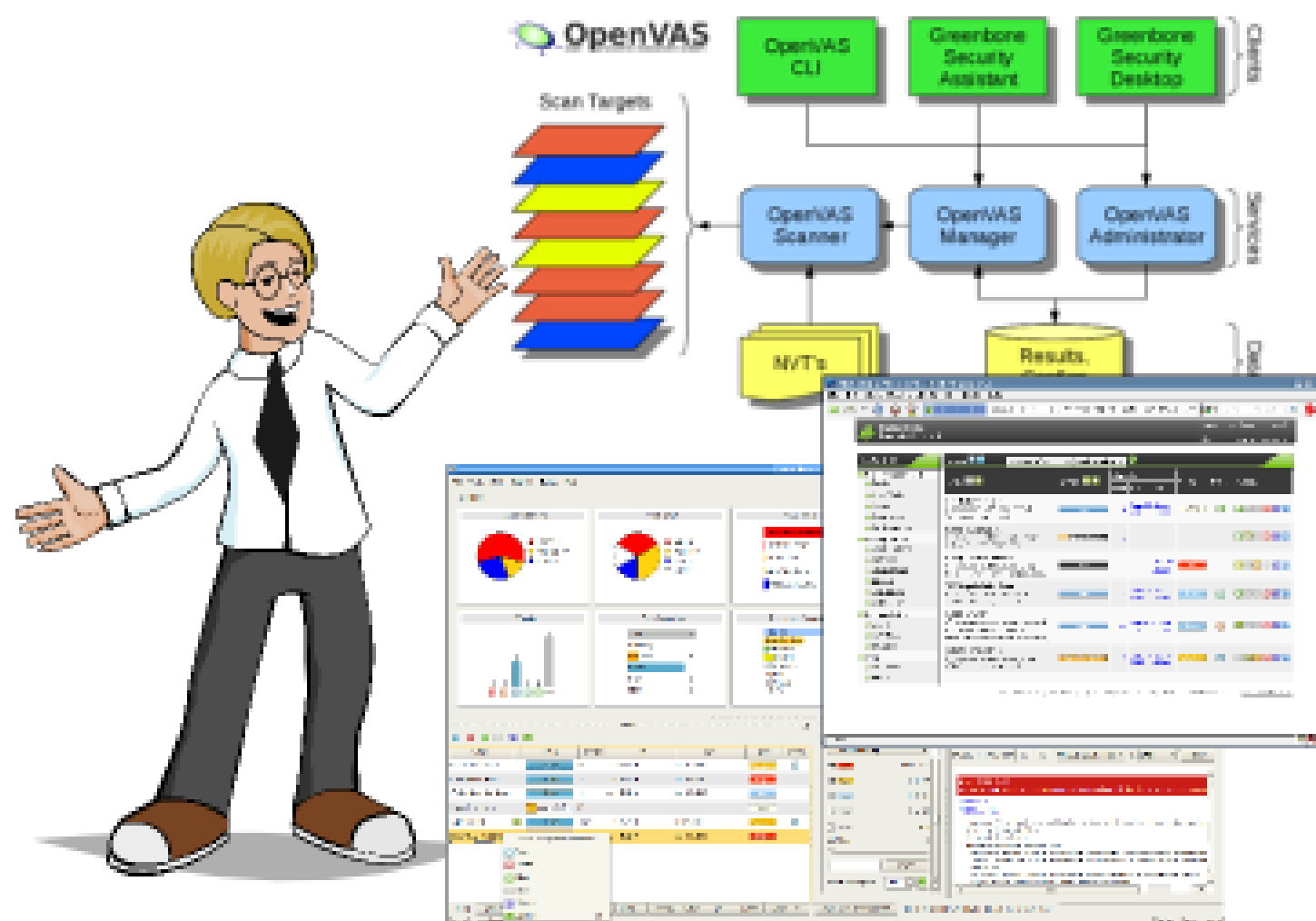
KALI LINUX™

“the quieter you become, the more you are able to hear”

EXPLOIT DATABASE



CAS D'UTILISATION



High (CVSS: 7.5)

http (80/tcp)

NVT: WordPress Spreadsheet plugin Multiple Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.804872)

Summary:

This host is installed with WordPress Spreadsheet plugin and is prone to multiple vulnerabilities.

Result:

Vulnerability detected.

Impact

Successful exploitation will allow remote attackers to execute arbitrary HTML and script code in a users browser session in the context of an affected site and inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

Impact Level: Application

Solution

No solution or patch is available as of 27th May, 2015. Information regarding this issue will be updated once the solution details are available. For updates refer http://timrohrer.com/blog/?page_id=71

Vulnerability Insight

Input passed via the 'ss_id' parameter to wpSS/ss_handler.php script is not validated before returning it to users.

Vulnerability Detection Method

Send a crafted data via HTTP GET request and check whether it is able to read cookie or not.

References

CVE: [CVE-2014-8363](#), [CVE-2014-8364](#)

BID: 69073, 69089

CERT: *Warning: database not available*

Other: <http://www.osvdb.com/109880>

<http://www.osvdb.com/109879>

<http://packetstormsecurity.com/files/127770>



QUESTIONS ?

Merci !