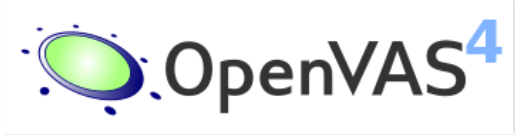
Vulnerability management with OpenVAS

Henri Doreau
henri.doreau@greenbone.net



12th LSM - Strasbourg
2011

Outline

Greenbone

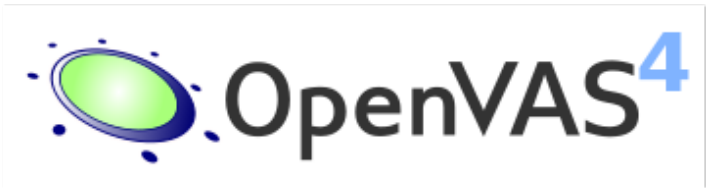
Outline

Greenbone

OpenVAS 4

The world most advanced Open Source vulnerability scanner!

⇒ 100% Free and Open Source Software (GPLv2)



`http://www.openvas.org`

Greenbone

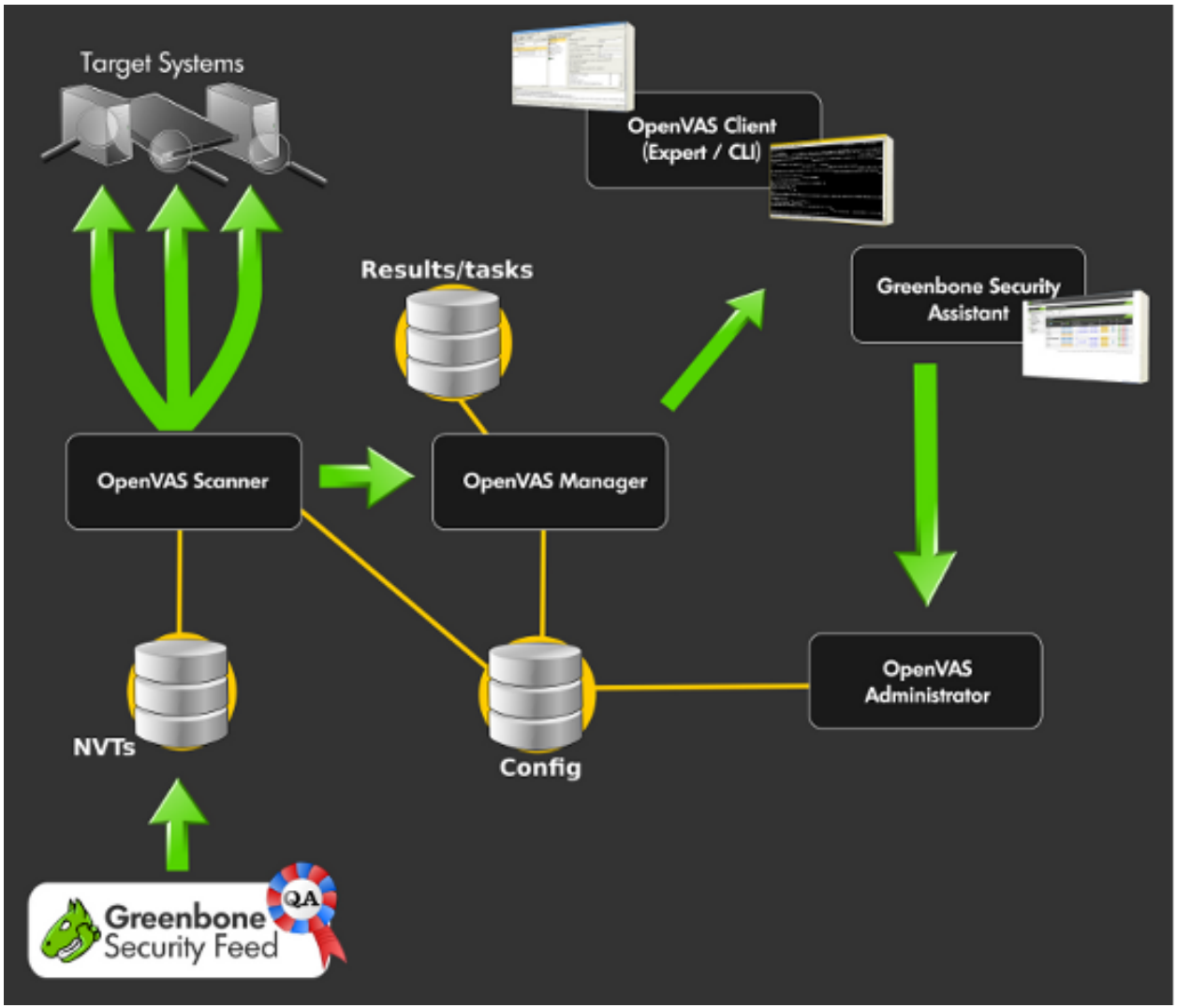
Vulnerability management

Day to day process to measure the IT threats of an infrastructure

- identify
- classify
- fix/mitigate

OpenVAS architecture

3-tiers scalable architecture



Greenbone

openvassd: scanning for vulnerabilities

Perform both authenticated and unauthenticated tests

Local Security Checks (LSC)

- information gathering
- missing updates/patches
- configuration correctness

⇒ over SSH

⇒ over SMB/WMI

Greenbone

openvassd: scanning for vulnerabilities

Perform both authenticated and unauthenticated tests

Local Security Checks (LSC)

- information gathering
- missing updates/patches
- configuration correctness

⇒ over SSH

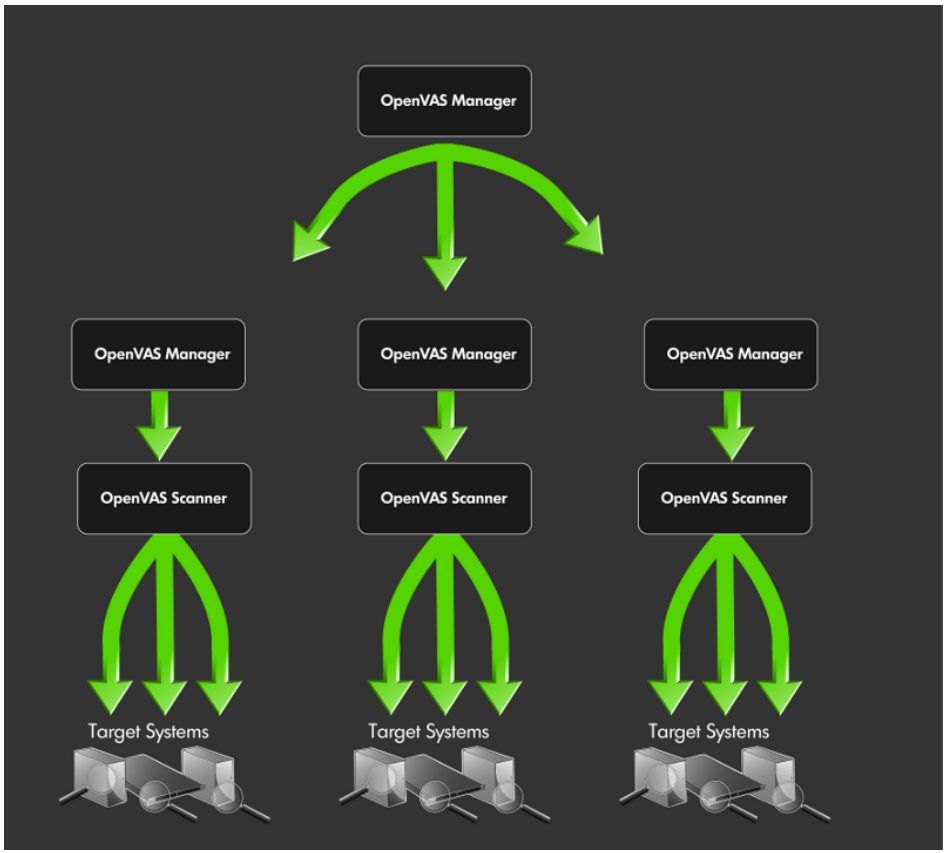
⇒ over SMB/WMI

Unauthenticated checks

- network scanning
- credentials bruteforce
- web applications audit

openvasmd: the network server

Handle scan information



- Scheduled tasks
- Scanning results
- Authentication

⇒ Ensure scalability

Greenbone

OpenVAS clients

Three clients available

- Portable (Qt) desktop client
- Web interface
- CLI for batch processing

Greenbone

OpenVAS clients

Three clients available

- Portable (Qt) desktop client
- Web interface
- CLI for batch processing
- python and ruby libraries (unofficial)

Greenbone

OpenVAS Ecosystem

Leverage specialized tools expertise

- nmap (general network scanning)
- ncrack (network authentication bruteforce tool)
- w3af, arachni, wapiti (web application audit)

OpenVAS Ecosystem

Uses and relies upon standards

- Common Vulnerability Enumeration
- Common Vulnerability Scoring System
- Common Platform Enumeration
- Open Vulnerability and Assessment Language
- IT-Grundschutz

Greenbone

What is OpenVAS not?

- OpenVAS is **not** an *automated pentester*
- OpenVAS is **not** an attack tool
- OpenVAS won't fix vulnerable systems

Greenbone

Outline

Greenbone

Aims

Keep threats under control

- Monitor patchlevel
- Detect insecure configurations
- Check for compliance with your security policy

⇒ Harden both the exposed perimeter and the core of the network.

Greenbone

Scan tasks

Task oriented workflow

- Targets
- Scan configuration
- Schedule
- Escalators

OpenVAS reports

Technical details and recommandations

High (CVSS: 10.0) http (80/tcp)
NVT: Heap-based buffer overflow in 'mbstring' extension for PHP (OID: 1.3.6.1.4.1.25623.1.0.900185)

```
Overview: The host is running PHP and is prone to Buffer Overflow
vulnerability.
Vulnerability Insight:
The flaw is caused due to error in mbfilter_htmlent.c file in the mbstring
extension. These can be exploited via mb_convert_encoding, mb_check_encoding,
mb_convert_variables, and mb_parse_str functions.
Impact:
Successful exploitation could allow attackers to execute arbitrary code via
a crafted string containing an HTML entity.
Impact Level: Application
Affected Software/OS:
PHP version 4.3.0 to 5.2.6 on all running platform.
Fix: Upgrade to version 5.2.7 or later,
http://www.php.net/downloads.php
References:
http://bugs.php.net/bug.php?id=45722
http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html
CVSS Score:
  CVSS Base Score     : 10.0 (AV:N/AC:L/Au:NR/C:C/I:C/A:C)
  CVSS Temporal Score : 7.4
Risk factor: High
CVE : CVE-2008-5557
BID : 32948
```

Greenbone

Questions OpenVAS aims to answer

What can OpenVAS actually do?

Greenbone

Questions OpenVAS aims to answer

Vulnerabilities

- Which ones?
- Where?
- How to fix/mitigate?

Questions OpenVAS aims to answer

Security policy

- Pass or fail?
- Does it need improvements?

Greenbone

Questions OpenVAS aims to answer

Security status

- Is it getting better or worse?
- How big is the risk?
- What to do first?

Greenbone

Outline

Greenbone

OpenVAS 4

"biggest step forward ever in the History"

- Massive code cleaning effort
- Report format plugins framework
- Scalable master-slave mode
- Performance increase (scan & analysis)
- Improved credentials management
- ...

Greenbone

OpenVAS 4

"biggest step forward ever in the History of OpenVAS"

- Massive code cleaning effort
- Report format plugins framework
- Scalable master-slave mode
- Performance increase (scan & analysis)
- Improved credentials management
- ...

Greenbone

OpenVAS 5

What's expected for OpenVAS 5?

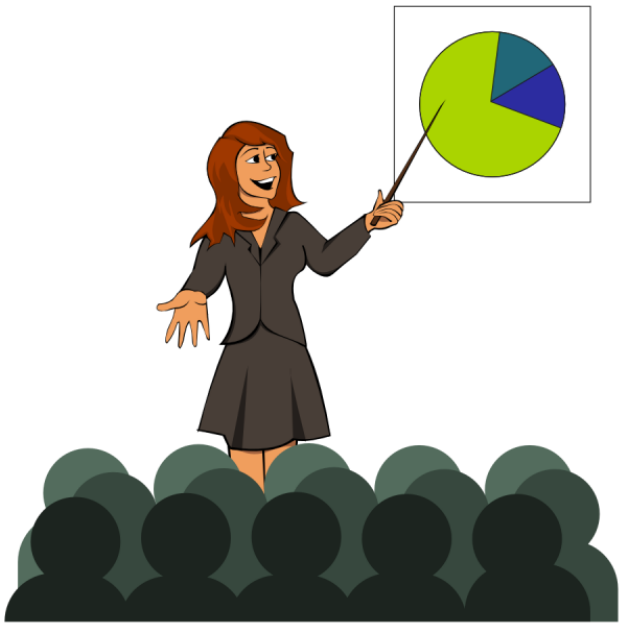
- High performance network scanning
- SSH stack refactoring
- Asset management
- Convenient trashcan
- Delta reports (diff scan results)

Greenbone

DevCon #3

bi-annual OpenVAS developers meeting

- Discussed core technology
- Identified priorities
- Established mid/long term projects
- Had great fun!



Greenbone

Demo

Questions?

http://www.openvas.org

openvas-discuss@wald.intevation.org