



Mauro Risonho de Paula Assumpção
Security Researcher
OpenVAS Project

In memorian



Alberto Fabiano Medeiros

in

br.linkedin.com/in/albertofabiano



Who i am?

1/21

- **Entusiasta em segurança**
- **Security Researcher OpenVAS Project** www.openvas.org
(desenvolvedor de plugins OpenVAS)
- **Moderador/Tradutor/Colaborador do Backtrack Linux**
www.backtrack-linux.org
- **Fundador do Backtrack Brasil** – Site não oficial (2008-2012)
www.backtrack.com.br (não tenho nada a ver com a equipe atual).
- **Palestrante na OWASP** www.owasp.org e ZapEvangelist do Zapproxy <https://code.google.com/p/zaproxy/wiki/ZapEvangelists>



Who i am?

2/21

- **Pesquisador OWASP OWTF** (Offensive (Web) Testing Framework, is an OWASP+PTES-focused)
- **Pesquisador PTES** (<http://www.pentest-standard.org/>) (aguardando ser adicionado ao projeto)
- Entusiasta da linguagem **Golang** www.golang.org (do Google)
- Pesquisador em segurança e Autodidata em geral.
- Nerd estilo década de 80 e minha esposa é “pin-up” estilo “geek” :)
- Um cara persistente em seus objetivos e metas e tem muito que aprender ainda...
- Sou “Risonho” e isso é obvio, vejam meu sobrenome !:)

SONHO DE CONSUMO
PROFISSIONAL ATUALMENTE^{3/21}

TRABALHAR
FULL TIME
EM
R&D

OpenVAS

4/21

- OpenVas começou GNessus, como um fork do Nessus, que era open source (GPL2) da Tenable Network Security e se tornou proprietário em outubro de 2005.
- OpenVAS foi originalmente modificado por pentesters no Portcullis Security, liderado por Tim Brown.

Estatísticas

5/21



<https://www.ohloh.net/p?q=openvas>

OpenVAS

Compare ☐



Analyzed 5 days ago

OpenVAS is an open source remote security vulnerability scanner, designed to search for networked devices and computers, discover accessible ports and services, and to test for vulnerabilities on any such ports; plugins allow for further expansion.

245K lines of code
18 current contributors
5 days since last commit
14 users on Ohloh

Very High Activity
 1 Review

[Mostly written in C](#)

[Licenses:](#) GPL-2.0+

network security vulnerability scanner

openvas-plugins

Compare ☐



Analyzed about 1 month ago

Network vulnerability tests collection for OpenVAS.

79 lines of code
11 current contributors
About 1 month since last commit
2 users on Ohloh

Activity Not Available
 0 Reviews

[Mostly written in shell script](#)

[Licenses:](#) GPL-2.0+

vulnerability network security scanner

Citações Internacionais 6/21

MITRE



<http://oval.mitre.org/adoption/participants.html#OpenVAS>

OpenVAS

Date Declared: July 6, 2012

Web Site: www.openvas.org

Quote/Declaration: OpenVAS is a vulnerability management and vulnerability scanning software framework. A feed service allows regular updates of Network Vulnerability tests (NVTs). The main security scan phase of the application collects security information about each host in the network being scanned. Subsequently, comprehensive OVAL-related processing is possible. This includes exporting system characteristics for the whole network, and applying the applications reporting framework according to OVAL Definitions.

PRODUCT NAME: [OpenVAS](#)

Type: Vulnerability Management

OVAL Authoring Tool: No

OVAL Definition Evaluator: Planned

OVAL Definition Repository: No

OVAL Results Consumer: Planned

OVAL System Characteristics Producer: Yes

[Review Completed Questionnaire](#)



Citações Internacionais 7/21

- http://iac.dtic.mil/csiac/download/vulnerability_assessment.pdf

IATAC



<http://iac.dtic.mil>

Open Vulnerability Assessment System 4

Abstract

The Open Vulnerability Assessment System (**OpenVAS**) is a framework of several custom-built and third-party services and tools that collectively implement a vulnerability scanning and vulnerability management solution. The included security scanner is updated daily through a feed of Network Vulnerability Tests; as of January 2011, the scanner supported 20,000 different vulnerability tests. **OpenVAS** Scanner can scan many target hosts concurrently, and can perform tests *via* an SSL session connection if necessary. **OpenVAS** Manager can manage multiple **OpenVAS** Scanners concurrently. It also provides management of scan results, including false positive verification and reduction, and scan operation (start, pause, stop, resume, scheduling). It also provides reporting capabilities, *via* plug-ins, in multiple formats, including (but not limited to) XML, HTML, and LaTeX. The **OpenVAS** Administrator enables configuration of the **OpenVAS** user accounts, and synchronization of its data feeds. All **OpenVAS** tools are accessible *via* Greenbone clients—either a remote client (that can be run from a thin/lean client with only a browser), a full desktop client

Open Vulnerability Assessment System 4

Type	Multilevel Scanner
Target(s)	Networks, Web applications
Format	Software, Appliance, or SaaS
OS	Linux (CentOS/Fedora/Red Hat/Debian/OpenSuSE/Ubuntu/Scientific Linux/Mandriva/Gentoo®/Slackware/SuSE Linux Enterprise/ArchLinux/BackTrack); FreeBSD; Windows
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Atomic Corporation's OpenVAS Project (Germany)
Information	http://www0.atomicorp.com/index.html

Citações Internacionais 8/21

<http://www.dfn-cert.de/en.html>



  | [Start » English](#)

[Startseite](#)

[Aktuelles](#)

[Unternehmen](#)

[Leistungen](#)

[Veranstaltungen](#)

[Informationen](#)

[Kontakt](#)

English

[CERT/CSIRT contact information](#)

[Imprint](#)

[RFC 2350](#)

English Pages

DFN-CERT offers consulting and services for improved Internet security. In particular, the protection of computers and computer networks from attacks and the security of electronic communications are the main tasks of DFN-CERT Services GmbH.

For this, DFN-CERT focuses security expertise in close cooperation with German and international computer emergency response teams (CERTs). This is where CERT advice and information from around the world comes together.

DFN-CERT has extensive experience in building and operating scalable and efficient security infrastructures. This includes the operation of advanced certification authorities (CAs).

In addition, DFN-CERT is involved in several research projects to develop and test new security technologies. We share our knowledge and experience in the form of expert advice, tutorials and workshops.

DFN-CERT - research, consultancy and services for improving Internet security.

- [CSIRT Description for DFN-CERT \(RFC 2350\)](#)
- [CERT/CSIRT contact](#)
- [Imprint](#)



Hier finden Sie Informationen zu den DFN-Diensten DFN-CERT und DFN-PKI.

[Veranstaltungen / Termine](#)

2. DFN-Workshop Datenschutz
Grand Elysee Hotel, Hamburg
10. - 11.12.2013

Tutorium "IT-Forensik und Vorfallsbehandlung in einem Linux-Umfeld"
Hamburg
09. - 10.01.2014

21. DFN-Workshop "Sicherheit in vernetzten Systemen"
Grand Elysee Hotel Hamburg
18. - 19.02.2014

Tutorium "Grundlagen der Forensik und Vorfallsbehandlung in einem Linux-Umfeld"
Grand Elysee Hotel, Hamburg
19.02.2014

Citações Internacionais 9/21

https://www.bsi.bund.de/DE/Home/home_node.html



Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt | Impressum | Service | RSS | Sitemap | English

[Das BSI](#) | [Themen](#) | [Aktuelles](#) | [Presse](#) | [Publikationen](#)



BSI-Informationen

[CERT-Bund](#)
[Cyber-Sicherheit](#)
[De-Mail](#)
[Elektronische Ausweise](#)
[IT-Grundschutz](#)
[IT-Lagezentrum](#)
[Kritische Infrastrukturen](#)
[Sicherheitsberatung](#)
[Zertifizierung und Anerkennung](#)

Suche 

IT-Sicherheit mitgestalten!
Stellenangebote des BSI

www.bmi.bund.de

[Startseite](#)
Kurzmitteilung
BSI zertifiziert TÜV Informationstechnik als IT-Sicherheitsdienstleister
Bonn, 28. November 2013.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die TÜV Informationstechnik GmbH als IT-Sicherheitsdienstleister im Geltungsbereich Penetrationstests zertifiziert. Das Zertifikat bestätigt, dass die Mitarbeiter der TÜV Informationstechnik GmbH befähigt sind, Sicherheitsuntersuchungen, Schwachstellenanalysen und Penetrationstests gemäß BSI-Standards bei Bundesbehörden durchzuführen, beziehungsweise die Dienstleistung BSI-konform anzubieten.

[Mehr >](#)

Pressemitteilung
BSI veröffentlicht „ICS Security Kompendium“
Grundlagenwerk zur Sicherheit industrieller Anlagen
Bonn, 26.11.2013.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem „ICS Security Kompendium“ ein Grundlagenwerk für die IT-Sicherheit in Automatisierungs-, Prozesssteuerungs- und Prozessleitsystemen (Industrial Control Systems, ICS) veröffentlicht. Das ICS Security Kompendium ermöglicht sowohl IT-Sicherheits- als auch ICS-Experten einen einfachen Zugang zum Thema IT-Sicherheit in industriellen Steuerungsanlagen. Es bildet den Rahmen für verschiedene Anwendungsbereiche industrieller Steuerungssysteme und dient als gemeinsame Basis für Experten in Anwendungsgebieten wie Fabrikautomation und Prozesssteuerung.

[Mehr >](#)

Kurzmitteilung
Mindeststandard TLS 1.2 und Web-Seiten des BSI
Bonn, 12.11.2013.

Schnell zu
[Mindeststandards](#)
SSL-TLS-Protokoll [FAQ](#)
Aufgaben und Themen des BSI
[IT-Grundschutz-Kataloge](#)
[Cyber-Sicherheit](#)
Sicherheitsberatung
Umsetzungsplan KRITIS
[De-Mail](#) [AusweisApp](#)
Smart Meter **CERT-Bund**

Allianz für Cyber-Sicherheit


BÜRGERCERT
Ins Internet - mit Sicherheit

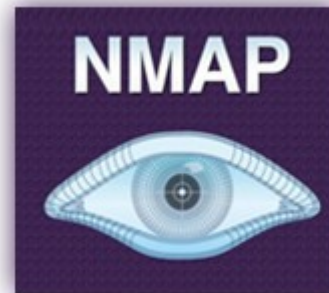
Arquitetura

10/21

- The Open Vulnerability Assessment System (OpenVAS) é um framework vários serviços e ferramentas.
- <http://www.openvas.org/integrated-tools.html>



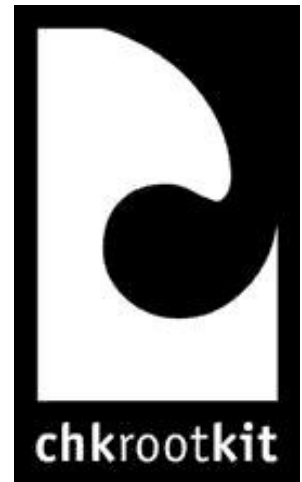
SNMPWALK



The Hacker's Choice

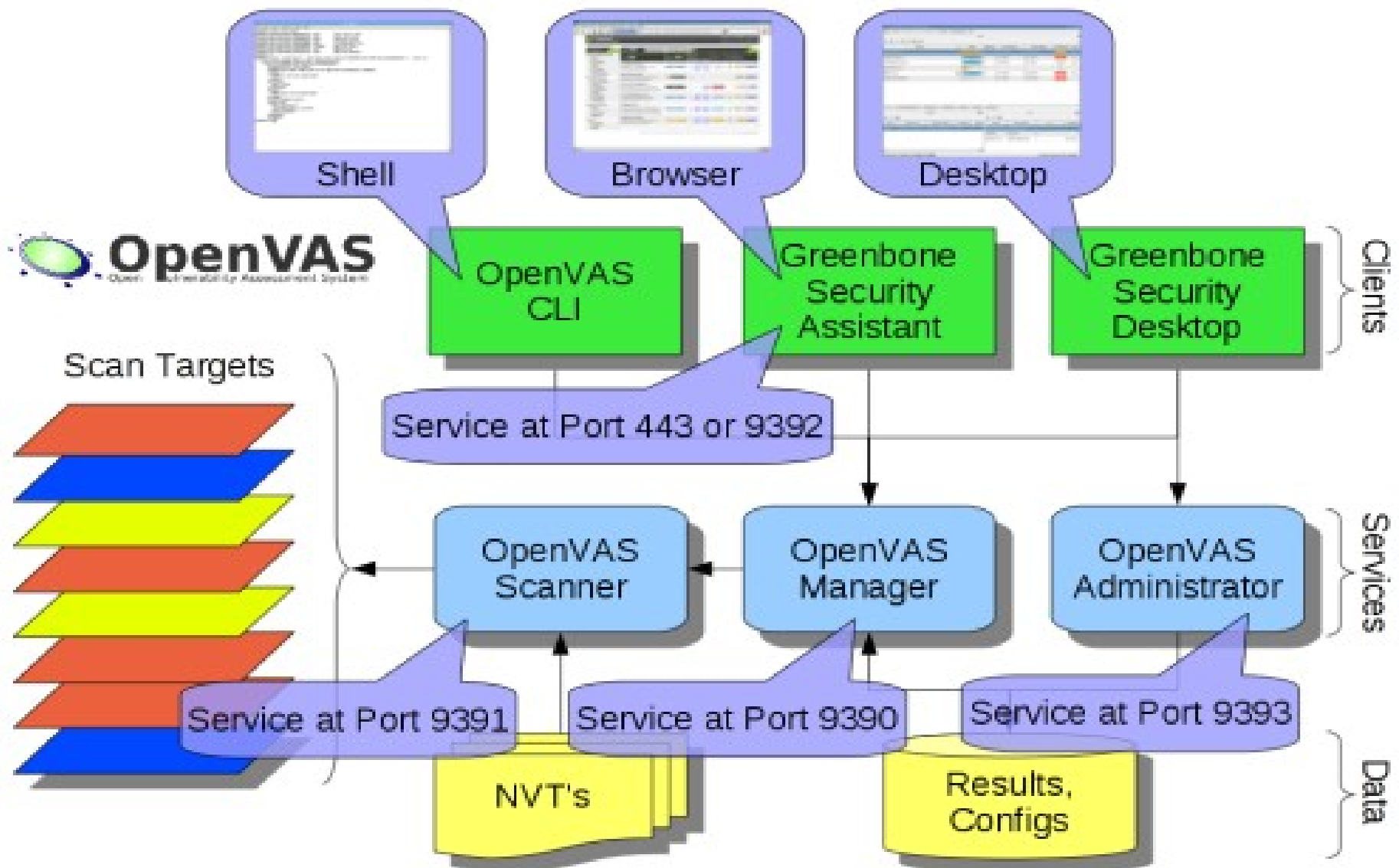


w3af
Web Application Attack and Audit Framework



Arquitetura

11/21



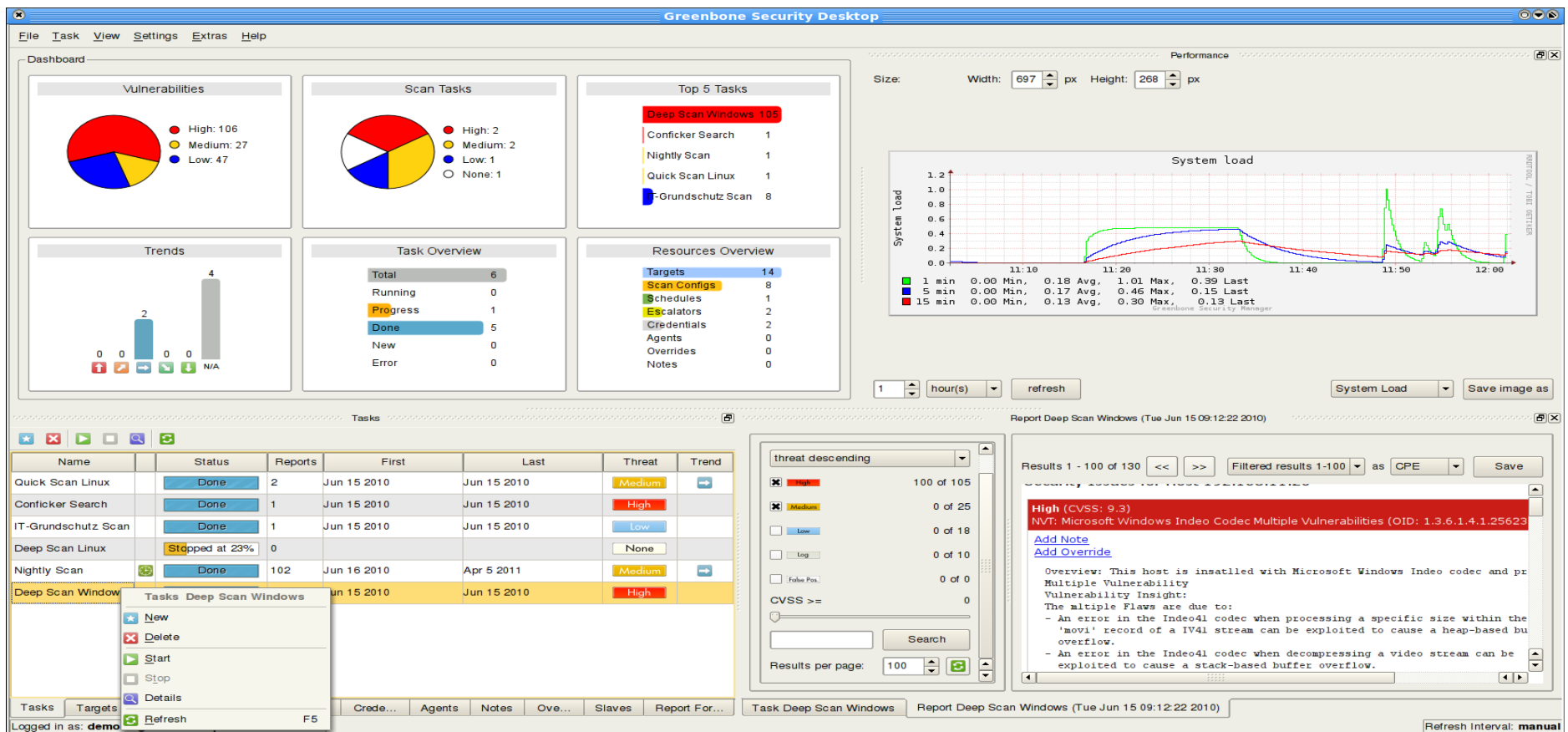
OpenVAS Manager

12/21

- The OpenVAS Manager é o serviço/gerenciador central que consolida as varreduras de vulnerabilidades e outras informações importantes durante o(s) scanning(s).

Greenbone Security Desktop (GSD) 13/21

- Greenbone Security Desktop (GSD) cliente desktop feito em Qt e que executa o protocolo OMP



OpenVAS Scanner

14/21

- The OpenVAS Scanner é o serviço/gerenciador central que consolida as varreduras de vulnerabilidades e outras informações importantes durante o(s) scanning(s).

OpenVAS CLI

15/21

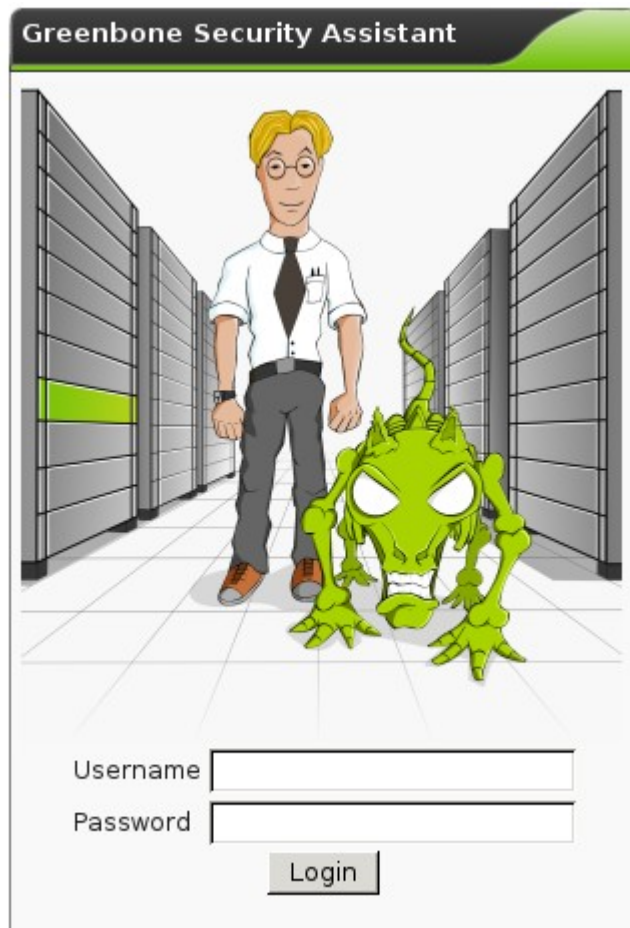
- OpenVAS CLI contém a ferramenta de linha de comando "omp" que permite criar processos batch para serem executados no OpenVAS Manager.

OpenVAS Administrator 16/21

- OpenVAS Administrator atua como uma ferramenta de linha de comando ou como um daemon de serviço que oferece o OpenVAS Administration Protocol (OAP). Este serviço é mais focado em Controle de acesso e administração de usuários que vão utilizar o OpenVAS

GSAD – Greenbone Security Assistant^{17/21}

- GSAD uma interface gráfica web, que atua para administração do OMP via web.



OpenVAS Administrator 18/21

- OpenVAS Administrator atua como uma ferramenta de linha de comando ou como um daemon de serviço que oferece o OpenVAS Administration Protocol (OAP).
- Este serviço é mais focado em Controle de acesso e administração de usuários que vão utilizar o OpenVAS

PLATAFORMAS/SERVERS ^{19/21} DEPLOYMENT



<http://www.openvas.org/install-packages.html>

Plugins NASL by firebits 20/21

- <https://github.com/firebitsbr/OpenVAS-Plugins-hardening/tree/master/plugins>
- svn checkout <https://scm.wald.intevation.org/svn/openvas-nvts>

Vulnerability Insight:

CVE-2010-0547 samba: mount.cifs improper device name and mountpoint strings sanitization

The MITRE CVE dictionary describes this issue as:

client/mount.cifs.c in mount.cifs in smbfs in Samba 3.4.5 and earlier does not verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string.

Affected Software/OS:

cifs on Red Hat Enterprise Linux version 4 (samba)

Fix: Please Install the Updated Packages.

References:

<https://access.redhat.com/security/cve/CVE-2010-0547>

<http://rpmfind.net/linux/rpm2html/search.php?query=samba”;>

if(description)

{

script_id(880323);

script_version("\$Revision: 12798 \$");

script_tag(name:"check_type", value:"authenticated package test");

script_tag(name:"last_modification", value:"\$Date: 2013-07-11 18:03:54 GMT-03:00 0 Brazil, São Paulo (Thu, 11 Jul 2013) \$");

script_tag(name:"creation_date", value:"2009-02-27 08:31:09 +0100 (Fri, 27 Feb 2009)");

script_tag(name:"cvss_base", value:"2.6");

script_tag(name:"cvss_base_vector", value:"AV:N/AC:L/Au:N/C:N/I:N/A:P");

script_tag(name:"risk_factor", value:"Low");

21/21



DEMO

PERGUNTAS ?



mauro.risonho@gmail.com



[http://br.linkedin.com/pub/mauro-risonho-de-paula-assump
%C3%A7%C3%A3o/b/b06/225/](http://br.linkedin.com/pub/mauro-risonho-de-paula-assump%C3%A7%C3%A3o/b/b06/225/)



<http://twitter/firebitsbr>



WORDPRESS <http://firebitsbr.wordpress.com/>

OBRIGADO PELA OPORTUNIDADE !



mauro.risonho@gmail.com



[http://br.linkedin.com/pub/mauro-risonho-de-paula-assump
%C3%A7%C3%A3o/b/b06/225/](http://br.linkedin.com/pub/mauro-risonho-de-paula-assump%C3%A7%C3%A3o/b/b06/225/)



<http://twitter/firebitsbr>



WORDPRESS <http://firebitsbr.wordpress.com/>