



**Greenbone**  
Sustainable Resilience

# Greenbone Vulnerability Manager (OpenVas)

La Mattina, Luca	-	57093
Reyes, Santiago	-	58148
Rolandelli, Alejandro	-	56644

# Introducción

## OpenVAS y Greenbone

- Open Source
- Escáner de vulnerabilidades
- Actualmente mantenido por Greenbone
- Junto con otros módulos Open Source forman el **Greenbone Vulnerability Management**

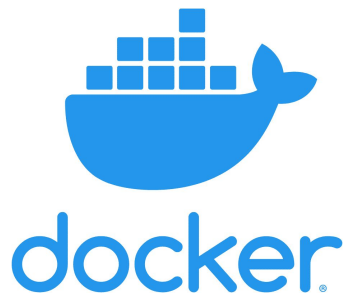
Greenbone ofrece soluciones enterprise para manejo de vulnerabilidades, como hardware o virtuales como modelo de negocios.

Nosotros usamos los módulos open source configurados en una imagen de Docker



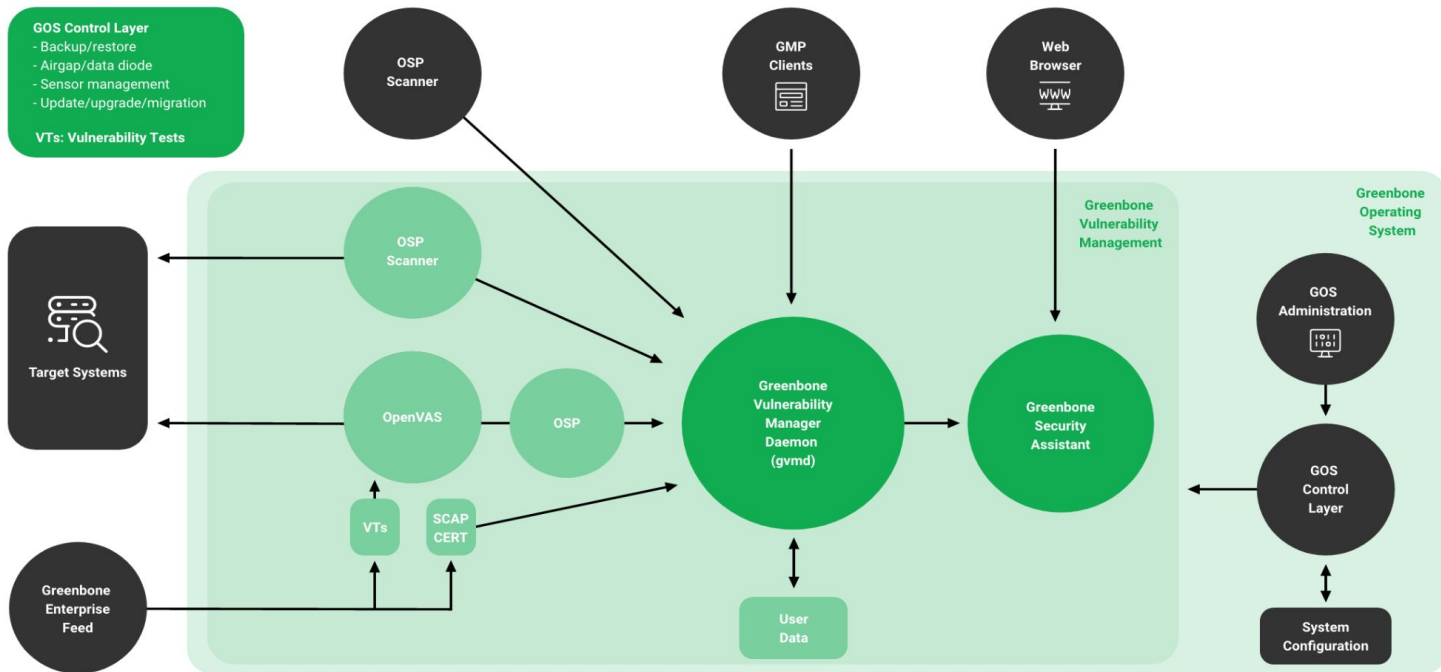
**OpenVAS by Greenbone**

Open Vulnerability Assessment Scanner



# Arquitectura

## Greenbone OS 20.08 and 21.04 Architecture



# Funcionalidades

---

**Escaneo de Redes  
(con o sin login)**

**Detección de  
vulnerabilidades, servicios  
y plataformas**

**Configuración de  
alertas**

---

**Creación y  
seguimiento de  
tickets**

**Generación de  
Reportes**

**Comparación de  
estados**

# NVT, CERT y SCAP

## ¿Qué son?

### NVT: Network Vulnerability Tests

Scripts para encontrar vulnerabilidades conocidas.

## ¿Cómo se usan?

GVM tiene una base de datos de NVTs, CVEs, CPEs y CERTs que se debe mantener actualizada.

OpenVAS las utiliza al escanear objetivos.



# NVT Ejemplo

## NVT: Mozilla Firefox Security Advisory (MFSA2011-22) - Linux

Information

Preferences  
(0)

User Tags  
(0)

### Summary

This host is missing a security update for Mozilla Firefox.

### Scoring

CVSS Base	10.0 (High)
CVSS Base Vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Origin	N/A
CVSS Date	Tue, Nov 16, 2021 11:08 AM UTC

### Insight

Integer overflow and arbitrary code execution in Array.reduceRight()  
Security researchers Chris Rohlf and Yan Ivnitkiy of Matasano Security reported that when a JavaScript Array object had its length set to an extremely large value, the iteration of array elements that occurs when its reduceRight method was subsequently called could result in the execution of attacker controlled memory due to an invalid index value being used to access element properties.


### Detection Method

Checks if a vulnerable package version is present on the target host.  
**Quality of Detection:** executable\_version\_unreliable (30%)

### Affected Software/OS

Firefox version(s) below 3.6.18 and below 5.

## Solution

**Solution Type:**  Vendorfix

The vendor has released an update. Please see the reference(s) for more information.

## Family

General

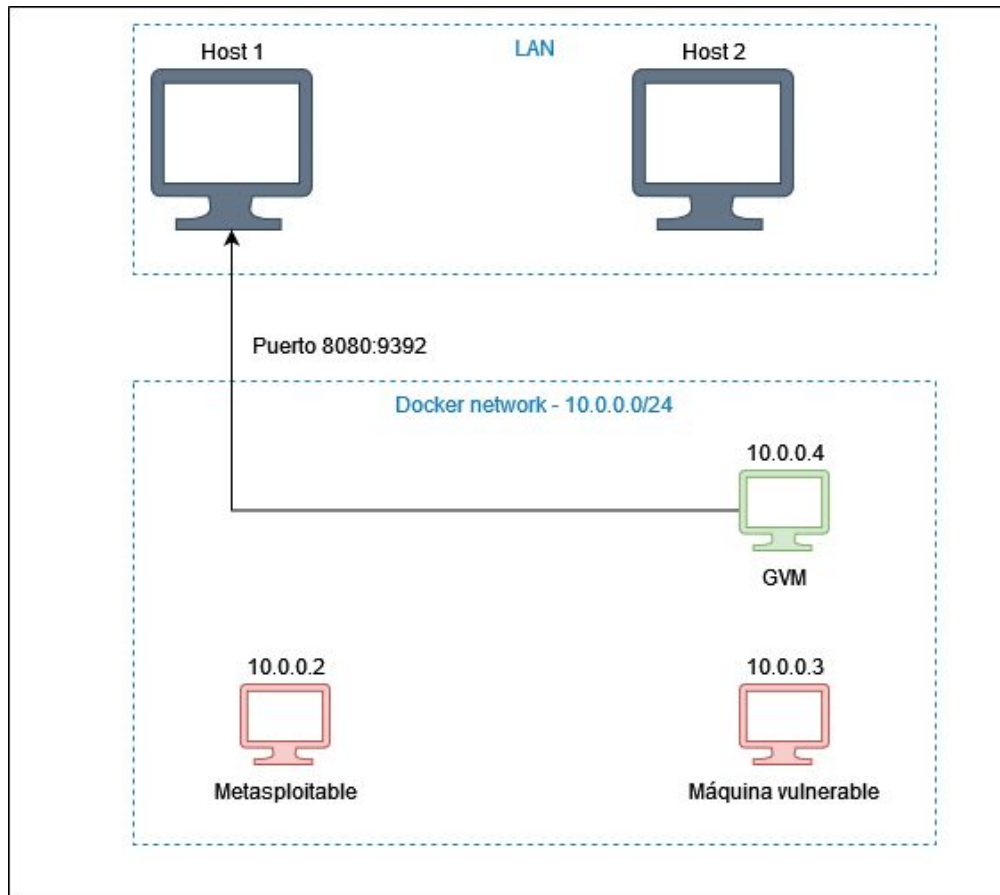
## References

CVE [CVE-2011-2371](#)

CERT [DFN-CERT-2012-0106](#)  
[DFN-CERT-2011-1080](#)  
[DFN-CERT-2011-1045](#)  
[DFN-CERT-2011-1032](#)  
[DFN-CERT-2011-1026](#)  
[DFN-CERT-2011-1013](#)  
[DFN-CERT-2011-1012](#)  
[DFN-CERT-2011-1007](#)  
[DFN-CERT-2011-1006](#)  
[DFN-CERT-2011-0991](#)  
[DFN-CERT-2011-0989](#)  
[DFN-CERT-2011-0980](#)  
[DFN-CERT-2011-0975](#)  
[DFN-CERT-2011-0974](#)  
[DFN-CERT-2011-0973](#)  
[DFN-CERT-2011-0971](#)

Other <https://www.mozilla.org/en-US/security/advisories/mfsa2011-22/>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=664009](https://bugzilla.mozilla.org/show_bug.cgi?id=664009)  
advisory-id: MFSA2011-22

# Topología



Se publica el puerto 9392 del contenedor GVM al puerto 8080 del host para poder acceder a la interfaz web desde el host1 en el puerto 8080.

El contenedor con GVM puede ver y escanear a los vulnerables, pero estos no son visibles desde fuera de la red virtual de docker.

# Contenedores Vulnerables

---

## Metasploitable

Máquina virtual con varios servicios vulnerables corriendo.

Hecha para probar herramientas de seguridad.

## Máquina vulnerable

Máquina virtual diseñada por nosotros.

Utiliza una versión desactualizada de Ubuntu y cuenta con un servicio ssh corriendo en el puerto 2222 con credenciales admin:admin.



# DEMO

