



CEP Lora del Río  
CONSEJERÍA DE EDUCACIÓN

# Curso de Seguridad y alta disponibilidad

CEP Lora del Río (Sevilla)

**PENTEST 2**



# Licencia

Estas diapositivas han sido realizadas para el curso “Seguridad y Alta Disponibilidad” que se imparte a través del CEP de Lora del Río (Sevilla).

© José Ignacio Huertas, Alberto Molina Coballes  
Septiembre 2013

Algunos derechos reservados. Este artículo se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en <http://creativecommons.org/licenses/by-sa/3.0/es/deed.es>





# Objetivos

## Objetivos de este segundo día:

1. Conocer los riesgos reales de seguridad.
2. Estudiar las distintas alternativas para la búsqueda de vulnerabilidades.
3. Utilizar software para búsqueda de bugs en nuestros equipos personales.
4. Utilizar escáner de vulnerabilidades (Nessus)



# Contenido del día 2

- **Análisis de vulnerabilidades:**
  - **Vulnerabilidades**
  - **Situación actual (Informe de seguridad Secunia 2013)**
  - **Comprobar vulnerabilidades en un equipo: Secunia PSI**
  - **Escáner de vulnerabilidades: Nessus**



# Vulnerabilidades

- Fallo en el diseño o configuración de un software.
- Genera un expediente de seguridad. Cada fabricante mantiene su forma de codificarlo.
- Hay empresas dedicadas a seguridad que mantienen bases de datos actualizadas con los expedientes:
  - Bugtraq: <http://securityfocus.com>
  - CVE (Common Vulnerabilities and Exposures):  
<https://cve.mitre.org/cve>
  - <https://secunia.com/advisories>



# Vulnerabilidades

Overview    Advisories    Research    Forums    Create Profile    Our Commitment

Database    Search    Advisories by Product    Advisories by Vendor    Terminology    Report Vulnerability    Insecure Library Loading

**Highly Critical**    **Oracle Java Multiple Vulnerabilities**

**Secunia Advisory SA53008**    **Release Date:** 2013-04-17    **Last Update:** 2013-05-30    **Views:** 25,431

**Where:** From remote

**Impact:** Security Bypass, Manipulation of data, Exposure of sensitive information, Privilege escalation, DoS, System access

**Solution Status:** Vendor Patch

**Software:**

- Oracle Java JDK 1.5.x / 5.x
- Oracle Java JDK 1.7.x / 7.x
- Oracle Java JRE 1.6.x / 6.x
- Oracle Java JDK 1.6.x / 6.x
- Oracle Java JRE 1.5.x / 5.x
- Oracle Java JRE 1.7.x / 7.x

**CVE Reference(s):**

<a href="#">CVE-2013-0401</a>	<a href="#">CVE-2013-0402</a>	<a href="#">CVE-2013-1488</a>	<a href="#">CVE-2013-1491</a>
<a href="#">CVE-2013-1518</a>	<a href="#">CVE-2013-1537</a>	<a href="#">CVE-2013-1540</a>	<a href="#">CVE-2013-1557</a>
<a href="#">CVE-2013-1558</a>	<a href="#">CVE-2013-1561</a>	<a href="#">CVE-2013-1563</a>	<a href="#">CVE-2013-1564</a>
<a href="#">CVE-2013-1569</a>	<a href="#">CVE-2013-2383</a>	<a href="#">CVE-2013-2384</a>	<a href="#">CVE-2013-2394</a>
<a href="#">CVE-2013-2414</a>	<a href="#">CVE-2013-2415</a>	<a href="#">CVE-2013-2416</a>	<a href="#">CVE-2013-2417</a>
<a href="#">CVE-2013-2418</a>	<a href="#">CVE-2013-2419</a>	<a href="#">CVE-2013-2420</a>	<a href="#">CVE-2013-2421</a>
<a href="#">CVE-2013-2422</a>	<a href="#">CVE-2013-2423</a>	<a href="#">CVE-2013-2424</a>	<a href="#">CVE-2013-2425</a>
<a href="#">CVE-2013-2426</a>	<a href="#">CVE-2013-2427</a>	<a href="#">CVE-2013-2428</a>	<a href="#">CVE-2013-2429</a>
<a href="#">CVE-2013-2430</a>	<a href="#">CVE-2013-2431</a>	<a href="#">CVE-2013-2432</a>	<a href="#">CVE-2013-2433</a>
<a href="#">CVE-2013-2434</a>	<a href="#">CVE-2013-2435</a>	<a href="#">CVE-2013-2436</a>	<a href="#">CVE-2013-2438</a>
<a href="#">CVE-2013-2439</a>	<a href="#">CVE-2013-2440</a>		



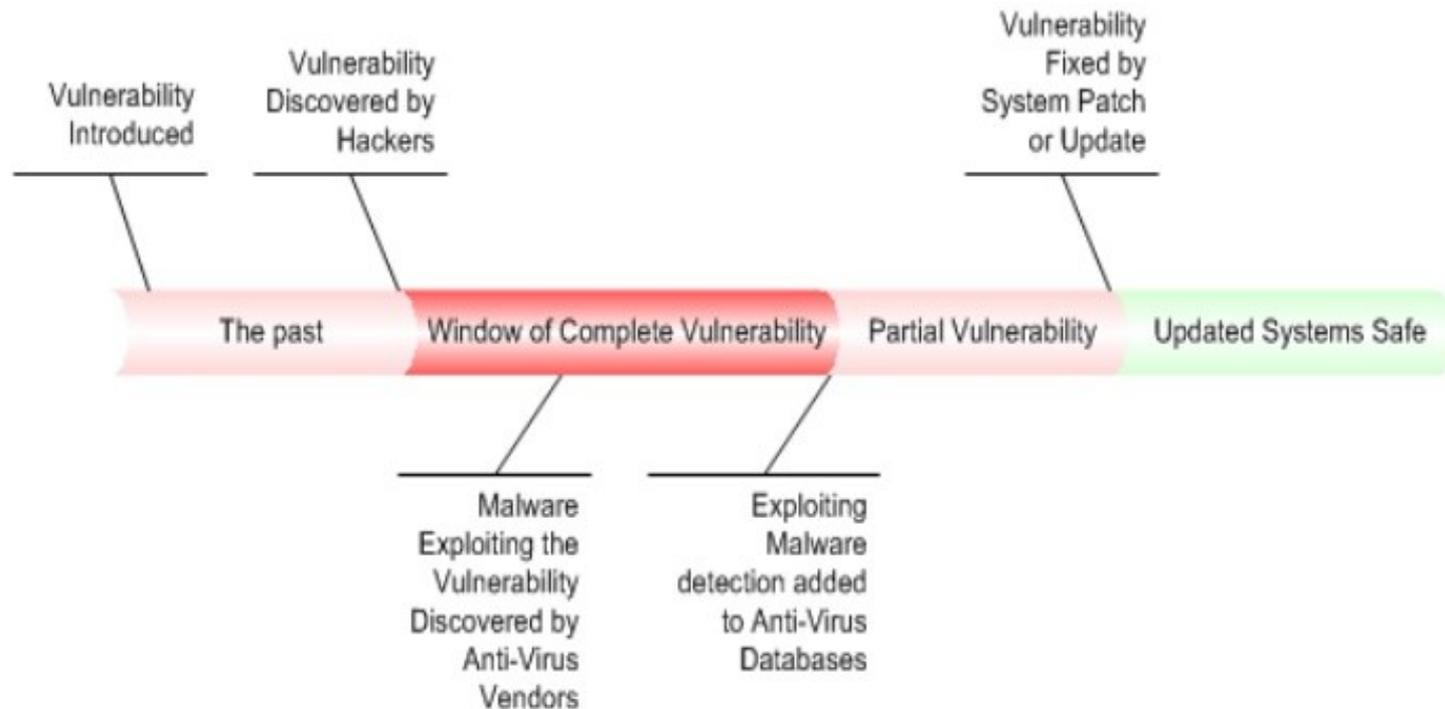
# Vulnerabilidades

- **Zero-day o día cero**, es el día en el que se hace pública una vulnerabilidad. A partir de este momento, el tiempo que se tarde en dar una solución será el **tiempo de reacción**.
- De este tiempo de reacción depende la probabilidad de que la vulnerabilidad descubierta sea explotada para configurar un ataque



# Vulnerabilidades

- Ciclo de vida de las vulnerabilidades





# Situación actual (Informe de seguridad Secunia 2013)

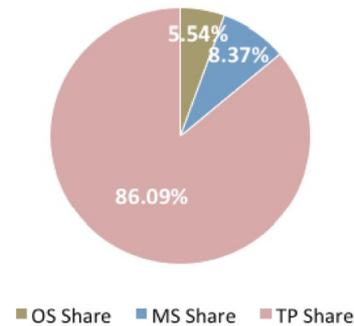
- Secunia: empresa referente en el sector de la seguridad informática.
- Emite informes anuales con estadísticas detalladas de seguridad. Gran parte de la información es recabada de los análisis que realiza su software.
- Mitos y leyendas.
- Los datos que se muestran a continuación han sido obtenidos de dicho informe.



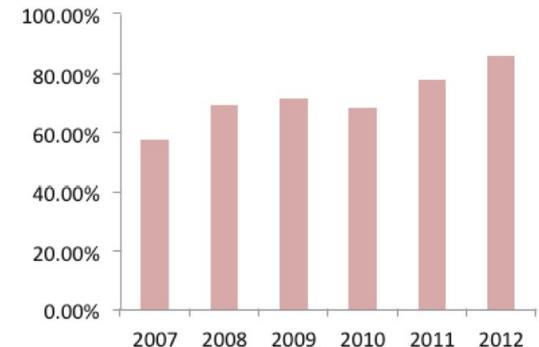
# Vulnerabilidades por tipos de programas

- Los programas de terceros superan en número de vulnerabilidades a los sistemas operativos Windows así como a los programas de Microsoft

Top-50 Portfolio  
share of vulnerabilities by source



Share of vulnerabilities  
by third-party programs

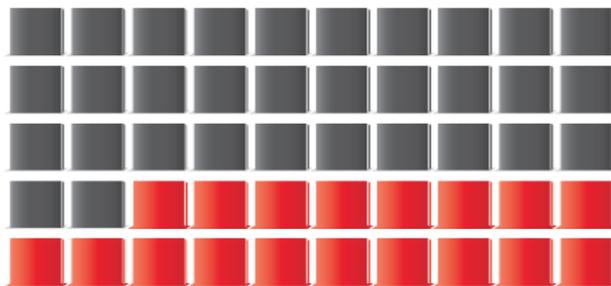




# ¿Quién tiene más vulnerabilidades?

## TOP 50

Vulnerabilities in the 50 most used programs (including Windows)



18 products had a total of 1,137 vulnerabilities  
(This number includes the operating system Windows 7)

GOOGLE CHROME	291
MOZILLA FIREFOX	257
APPLE ITUNES	243
ADOBE FLASH PLAYER	67
ORACLE JAVA JRE SE	66
ADOBE AIR	56
MICROSOFT WINDOWS 7	50
ADOBE READER	43
MICROSOFT INTERNET EXPLORER	41
APPLE QUICKTIME	29
MICROSOFT .NET FRAMEWORK	14
VLC MEDIA PLAYER	11
MICROSOFT EXCEL	10
MICROSOFT VISIO VIEWER	7
MICROSOFT SILVERLIGHT	5
MICROSOFT WORD	3
SKYPE	1
MICROSOFT XML CORE SERVICES (MSXML)	1

In the top 50 portfolio the total number of end-point vulnerabilities in 2012 was

# 1137

In the 5 year trend, this shows an increase of

# 98%

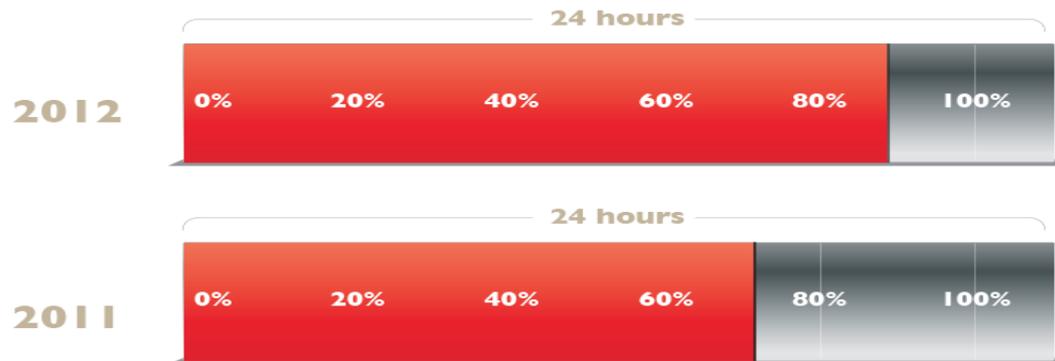
The 1,137 vulnerabilities were discovered in 18 of the Top 50 products - an average of 63 vulnerabilities per product.



# ¿Tardan mucho en salir los parches?

TOP 50

When are patches available for vulnerabilities in the Top 50 programs?



**84%**

of vulnerabilities had patches available on the day of disclosure in 2012

**72%**

of vulnerabilities had patches available on the day of disclosure in 2011

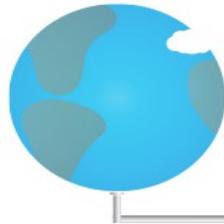


# ¿Desde dónde se ataca?

TOP 50

These are the attack vectors used by attackers to trigger or reach a vulnerability in a program

**Remote network**



**91%** Remote network used as attack vector

**Your local network**



**2%** Local network used as attack vector

**Your computer**



**7%** Local system used as attack vector

The majority of attacks are carried out by a hacker from a remote network, where the attacker is not required to have access to the system or a local network in order to exploit the vulnerability.



# Comprobar vulnerabilidades

- Secunia PSI (Personal Software Inspector) es gratuito (de uso personal) y nos permite comprobar el estado de actualización del sistema operativo así como de todas las aplicaciones instaladas, verificando también si existen vulnerabilidades en nuestra máquina.
- ¿Lo probamos?



# Escáner de vulnerabilidades

- ¿Y si quiero escanear más máquinas en mi organización?.
- Un escáner de vulnerabilidades es un programa diseñado para buscar de forma automática debilidades en ordenadores, sistemas, redes y aplicaciones.
- El programa prueba un sistema enviando datos a través de la red y analiza las respuestas recibidas, tratando de enumerar las vulnerabilidades presentes en el sistema objetivo usando su base de datos de vulnerabilidades como referencia para generar un informe con toda la información.
- Es posible utilizar un conjunto de credenciales para logearse en los sistemas de forma que se lista el software y los servicios instalados, determinando si están parcheados.

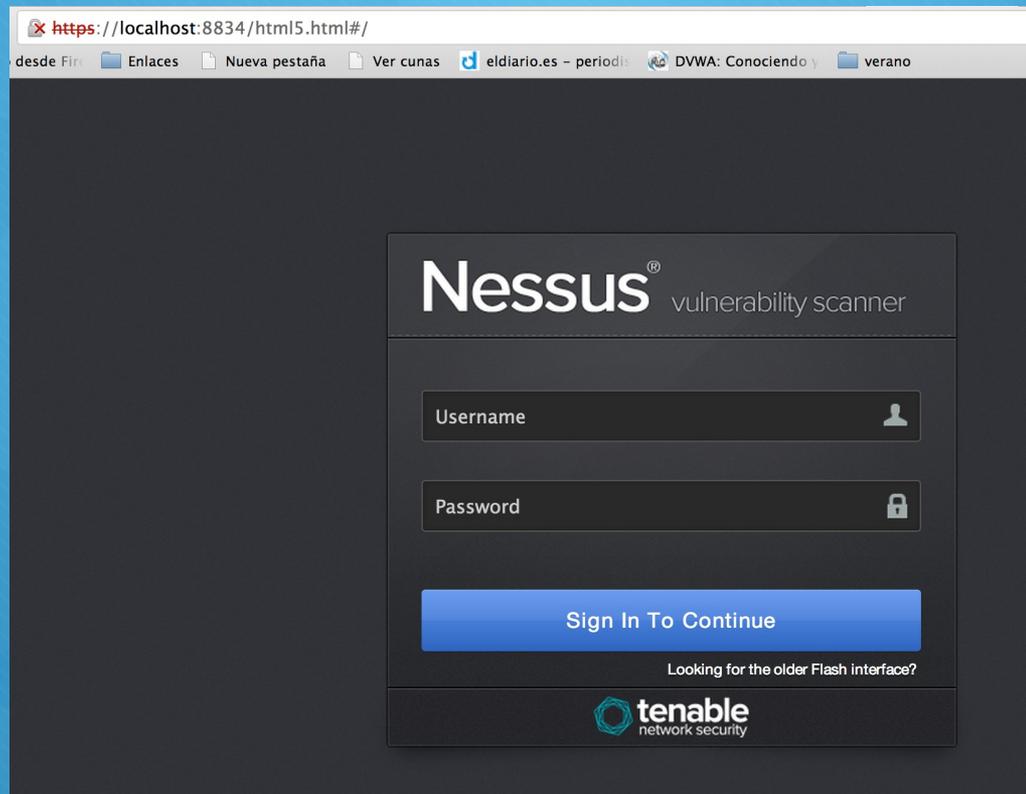


# Escáner de vulnerabilidades

- Software para escanear en red:
  - Nessus
  - OpenVas
  - Retina
  - NeXpose
  - Secunia SmallBusiness o CSI
  - ...



# Nessus: escaneando la red



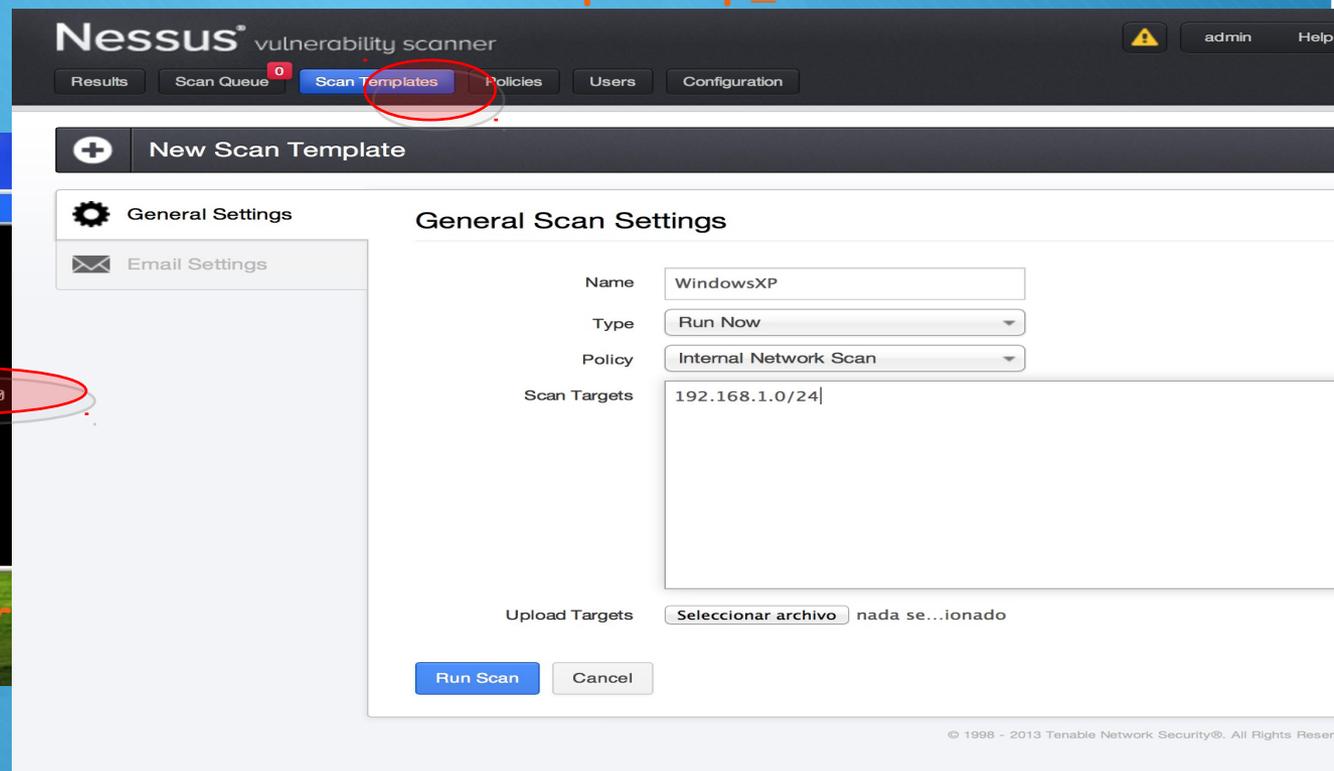
The screenshot shows a web browser window with the URL `https://localhost:8834/html5.html#/`. The browser's address bar and tabs are visible. The main content area displays the Nessus login interface, which includes the following elements:

- Header:** "Nessus<sup>®</sup> vulnerability scanner" in white text on a dark background.
- Username Field:** A text input field with a user icon on the right.
- Password Field:** A text input field with a lock icon on the right.
- Sign In Button:** A prominent blue button with the text "Sign In To Continue".
- Footer:** A link that says "Looking for the older Flash interface?" and the Tenable Network Security logo.



# Nessus: escaneando la red

[https://<ip\\_nessus>:8834](https://<ip_nessus>:8834)



The screenshot shows the Nessus vulnerability scanner web interface. The top navigation bar includes 'Results', 'Scan Queue', 'Scan Templates' (highlighted with a red circle), 'Policies', 'Users', and 'Configuration'. The main content area is titled 'New Scan Template' and contains two sections: 'General Settings' and 'Email Settings'. The 'General Settings' section includes a 'General Scan Settings' form with the following fields:

- Name: WindowsXP
- Type: Run Now
- Policy: Internal Network Scan
- Scan Targets: 192.168.1.0/24
- Upload Targets: Seleccionar archivo nada se...ionado

At the bottom of the form are 'Run Scan' and 'Cancel' buttons. The footer of the page reads '© 1998 - 2013 Tenable Network Security®. All Rights Reserved'.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\>ipconfig

Configuración IP de Windows

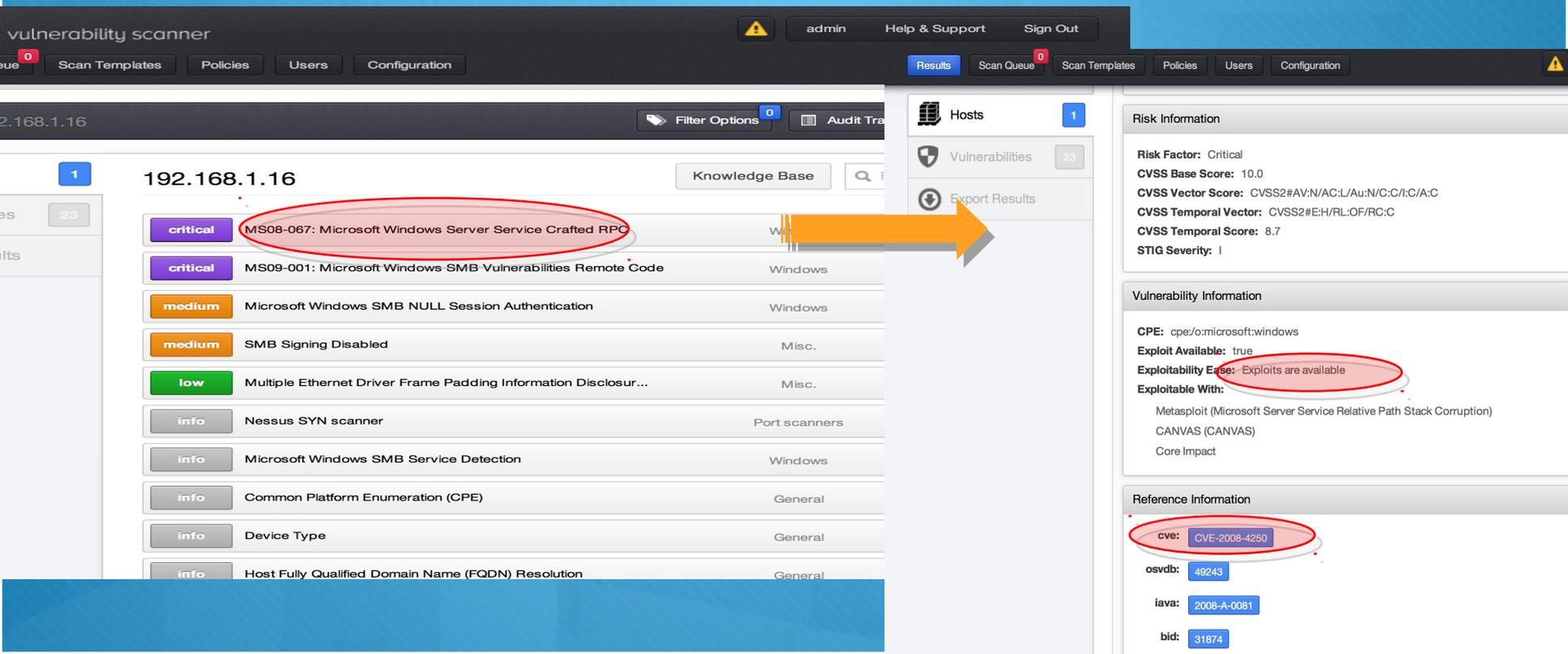
Adaptador Ethernet Conexión de área local :
Sufrido de conexión específica DNS : home
Dirección IP. . . . . : 192.168.1.16
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1

F:\pijota>
```

Equipo a escanear



# Nessus: informe de resultados



vulnerability scanner

admin Help & Support Sign Out

Scan Templates Policies Users Configuration

Results Scan Queue Scan Templates Policies Users Configuration

192.168.1.16

Filter Options Audit Trail Knowledge Base

Severity	Vulnerability Name	Category
critical	MS08-067: Microsoft Windows Server Service Crafted RPC	Windows
critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code	Windows
medium	Microsoft Windows SMB NULL Session Authentication	Windows
medium	SMB Signing Disabled	Misc.
low	Multiple Ethernet Driver Frame Padding Information Disclosur...	Misc.
info	Nessus SYN scanner	Port scanners
info	Microsoft Windows SMB Service Detection	Windows
info	Common Platform Enumeration (CPE)	General
info	Device Type	General
info	Host Fully Qualified Domain Name (FQDN) Resolution	General

Hosts 1

Vulnerabilities 28

Export Results

Risk Information

Risk Factor: Critical  
CVSS Base Score: 10.0  
CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  
CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C  
CVSS Temporal Score: 8.7  
STIG Severity: I

Vulnerability Information

CPE: cpe/o:microsoft:windows  
Exploit Available: true  
Exploitability Ease: Exploits are available  
Exploitable With:  
Metasploit (Microsoft Server Service Relative Path Stack Corruption)  
CANVAS (CANVAS)  
Core Impact

Reference Information

cve: CVE-2008-4250

osvdb: 49243

iava: 2008-A-0081

bid: 31874



# Openvas

https 192.168.1.18:9392/omp?cmd=get\_tasks&overrides=1&token=d9f6ec9d-fc42-4dbc-b517-a54fa8ad558b — Greenbone Security Assistant

**Greenbone Security Assistant** Logged in as Admin **admin** | Logout  
Sun Sep 8 08:20:34 2013 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 1 of 1 (total: 1) ? ✖ ☰ ↓ √No auto-refresh √Apply overrides ↻

Filter:  ? + -- + ?

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
Immediate scan of IP 192.168.1.19	Done	1	Sep 8 2013	Medium		<span>▶</span> <span>▶▶</span> <span>⏸</span> <span>🗑️</span> <span>🔍</span> <span>🔗</span> <span>👤</span> <span>⬇️</span>	

(Applied filter: apply\_overrides=1 first=1 rows=10 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.

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net



# TAREA: ¿Tienes vulnerabilidades?

- Utilizando algún escáner de los vistos, realiza la búsqueda de vulnerabilidades en alguna máquina e interpreta los resultados.
- Corrige todo lo que puedas y vuelve a pasar el escáner.
- Comparte los resultados en el foro del curso.



# Lecturas recomendadas:

- [http://secunia.com/?action=fetch&filename=Secunia\\_Vulnerability\\_Review\\_2013.pdf](http://secunia.com/?action=fetch&filename=Secunia_Vulnerability_Review_2013.pdf)
- <http://www.slideshare.net/jmorenol/sad-tema1-introduccionii1213>