JUNTA DE ANDALUCIA

CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Curso de Seguridad y alta disponibilidad

CEP Lora del Río (Sevilla)

PENTEST 2

JUNTA DE ANDALUCIA
CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

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).

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)

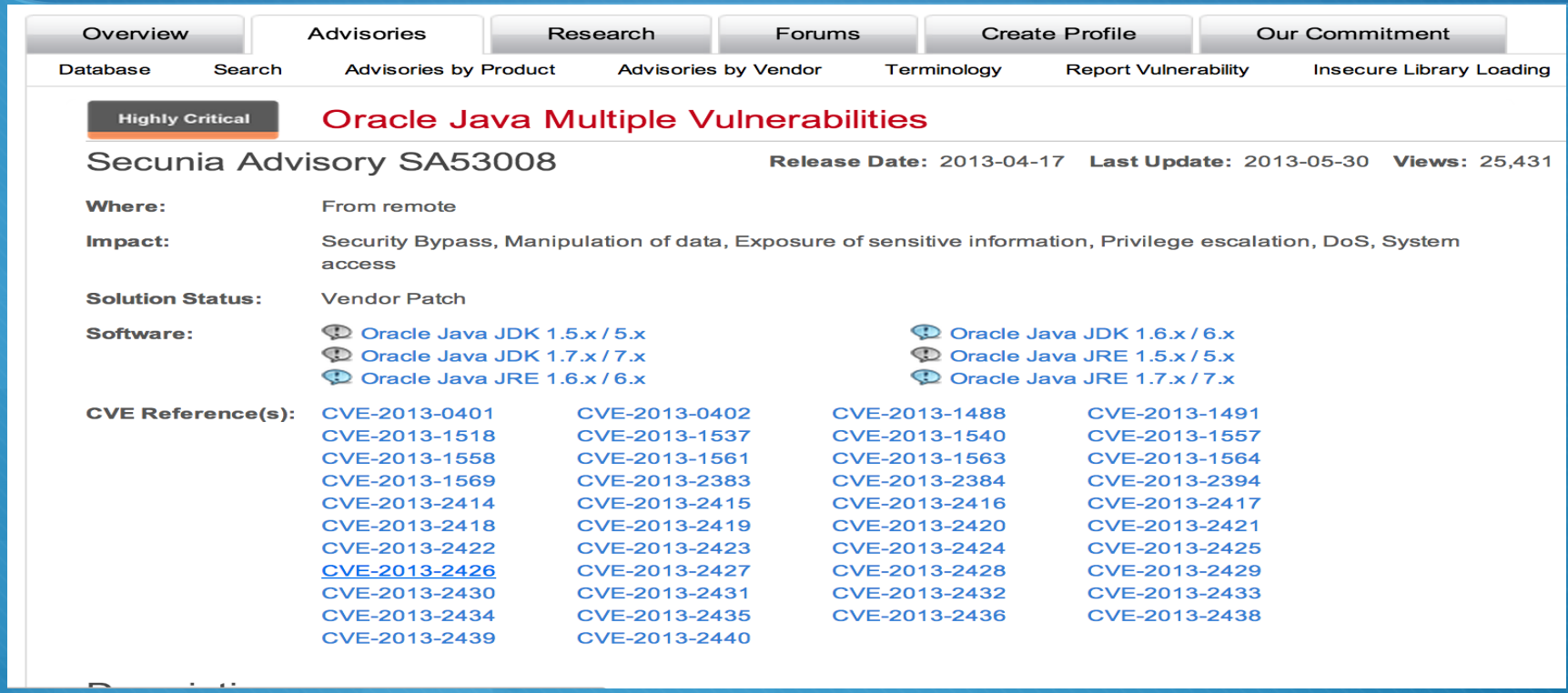
Contenido del día 2

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

CVE Reference(s):

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

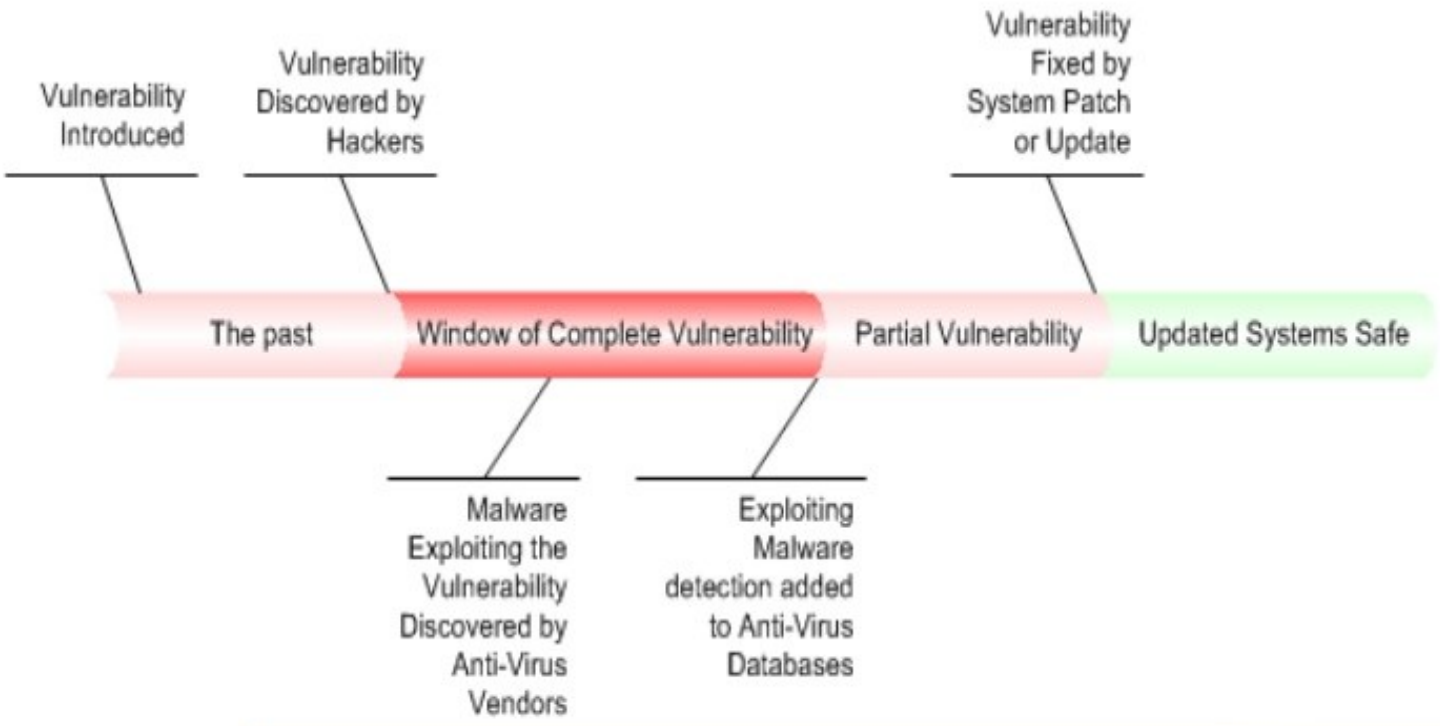
http://secunia.com/advisories/53008/

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

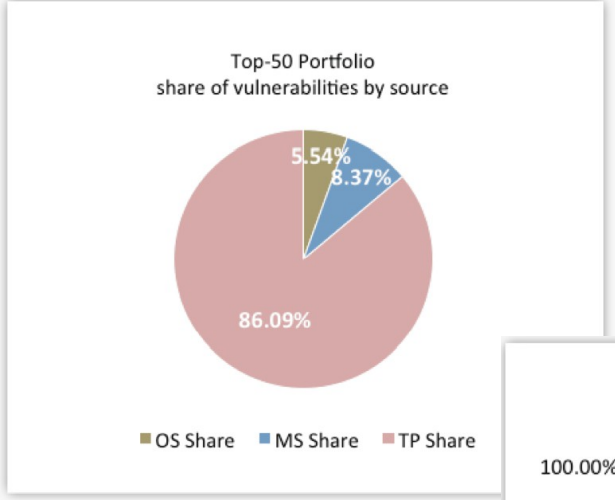


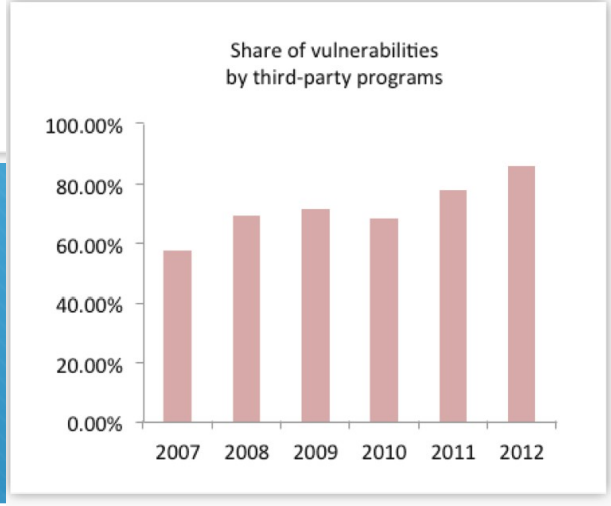
Situación actual (Informe de seguridad Secunia 2013)

- 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

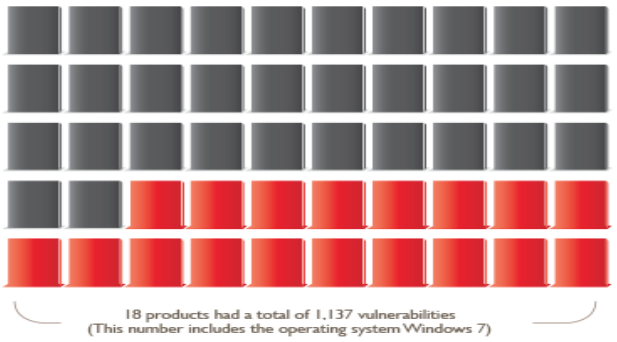




¿Quién tiene más vulnerabilidades?

TOP 50

Vulnerabilities in the 50 most used programs (including Windows)



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

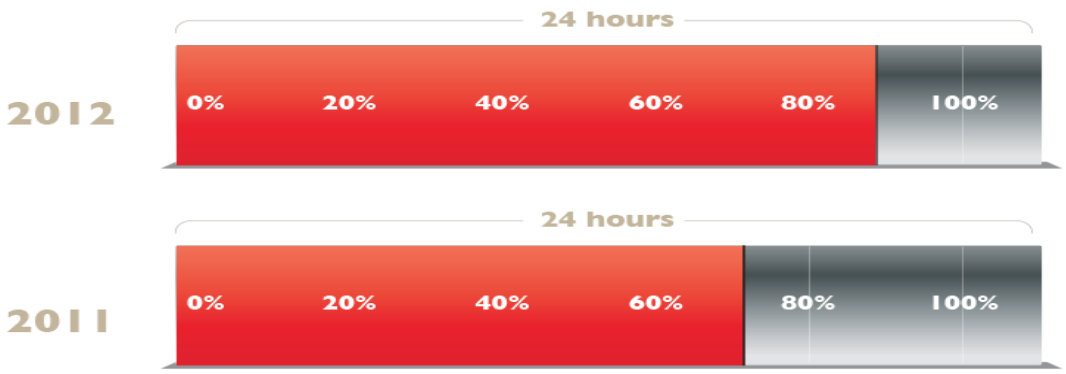
98%

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?



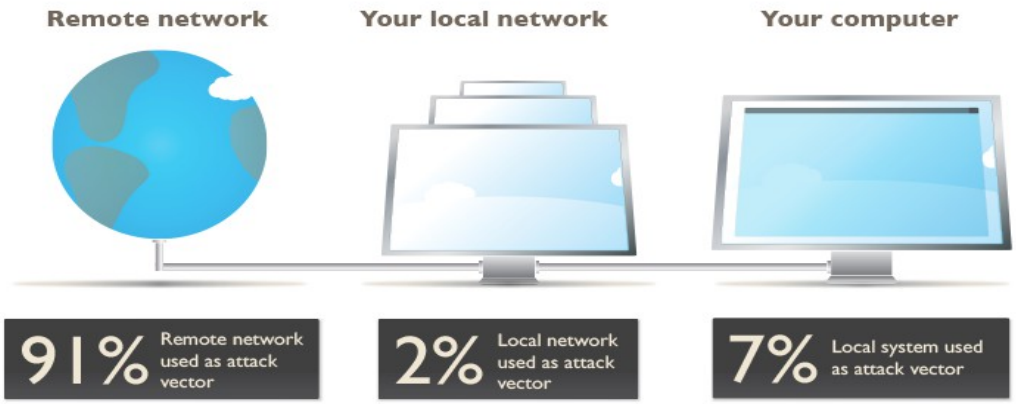
84% of vulnerabilities had patches available on the day of disclosure in 2012

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



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?

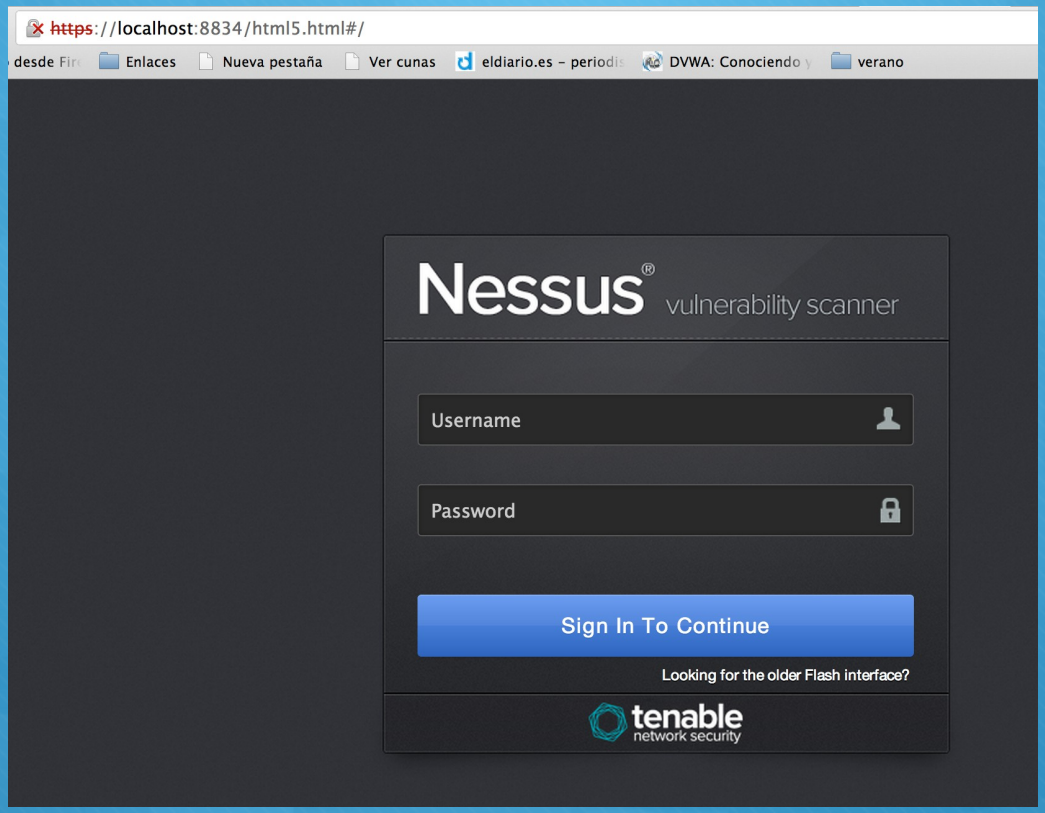
Escáner de vulnerabilidades

- ¿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
  - ...

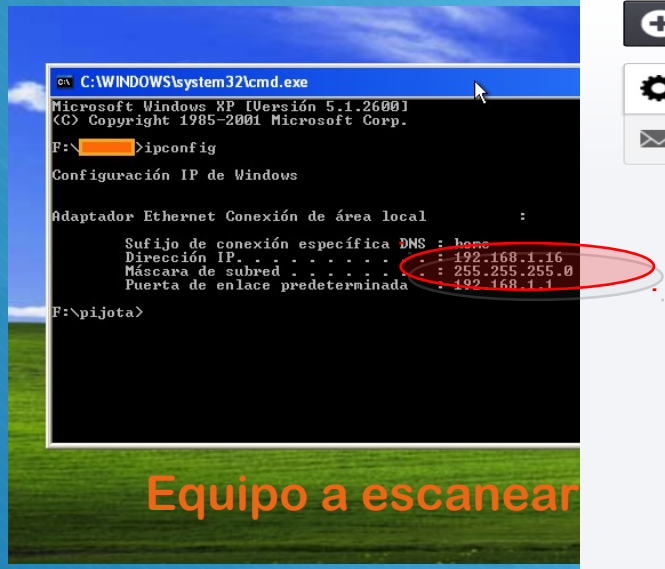
Nessus: escaneando la red

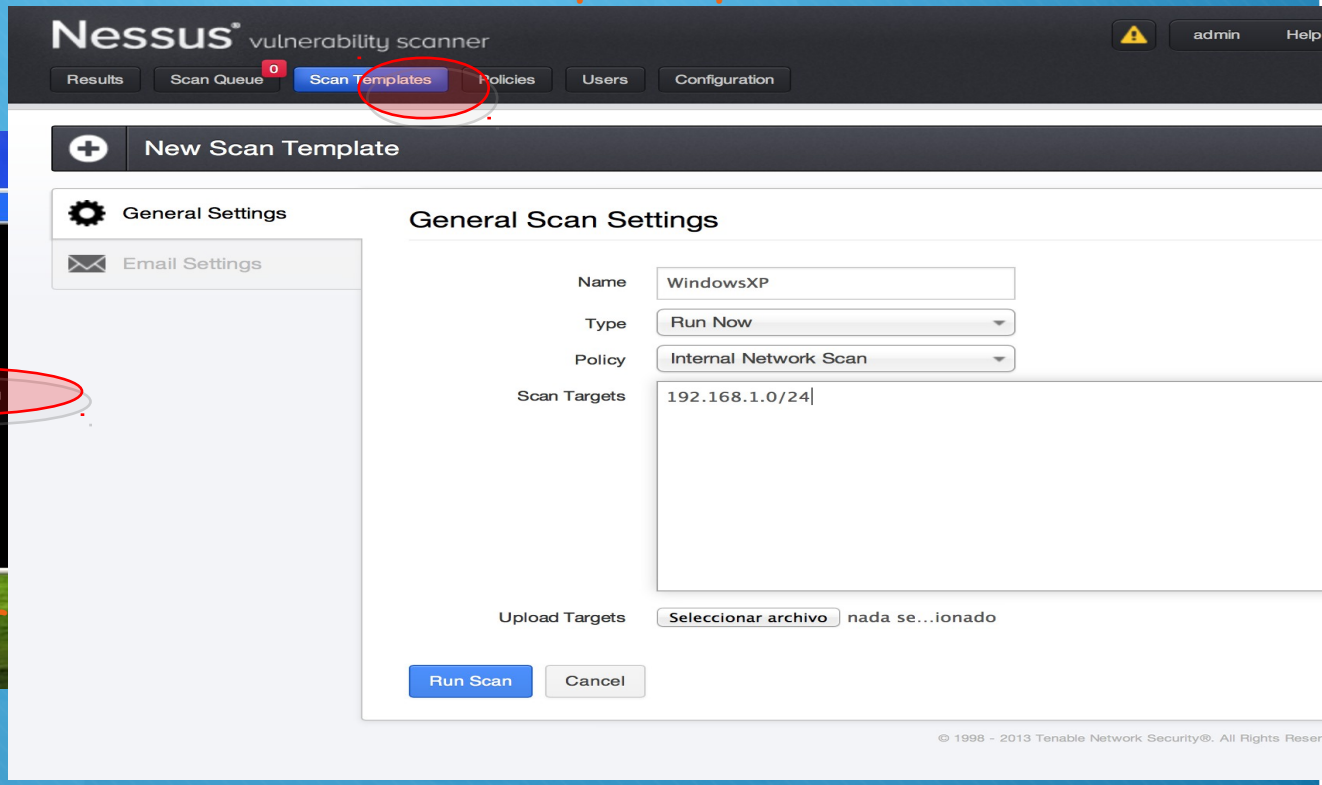


JUNTA DE ANDALUCIA
CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Nessus: escaneando la red

https://<ip_nessus>:8834

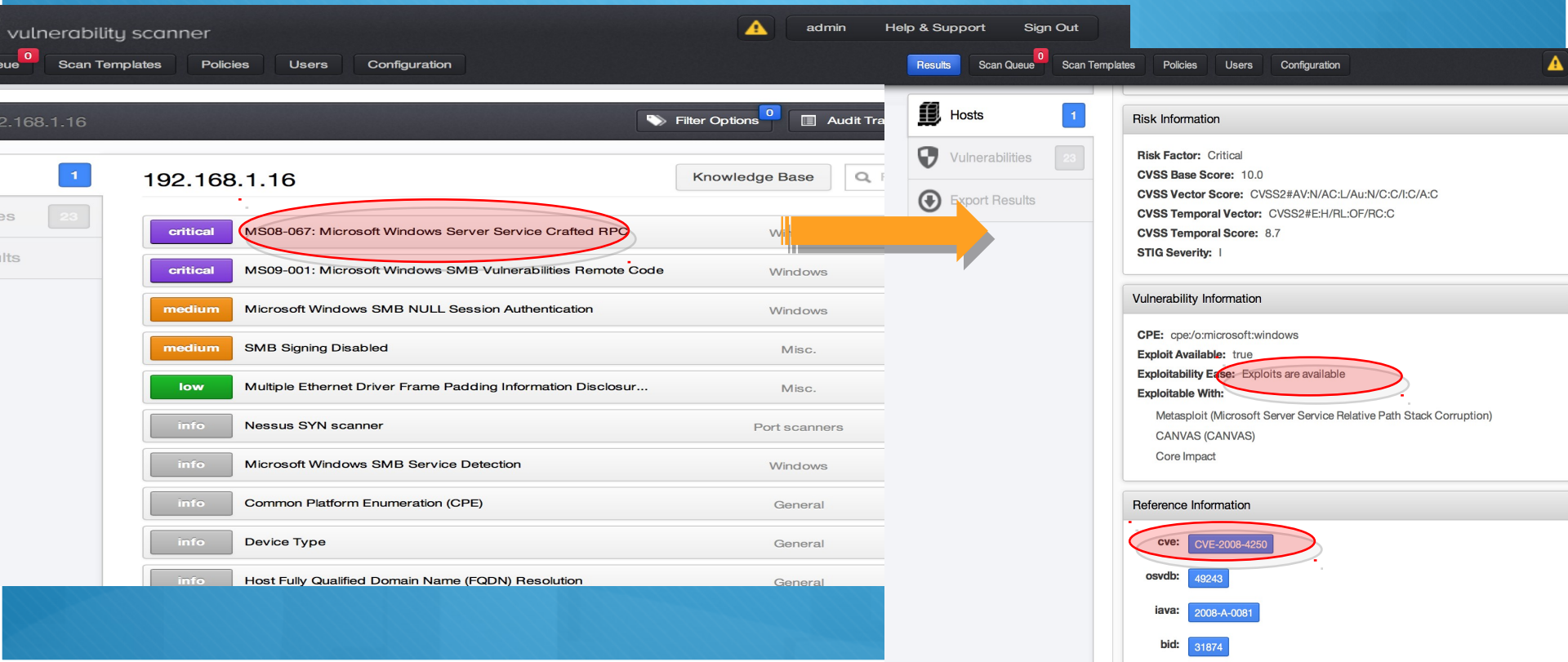




JUNTA DE ANDALUCIA

CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

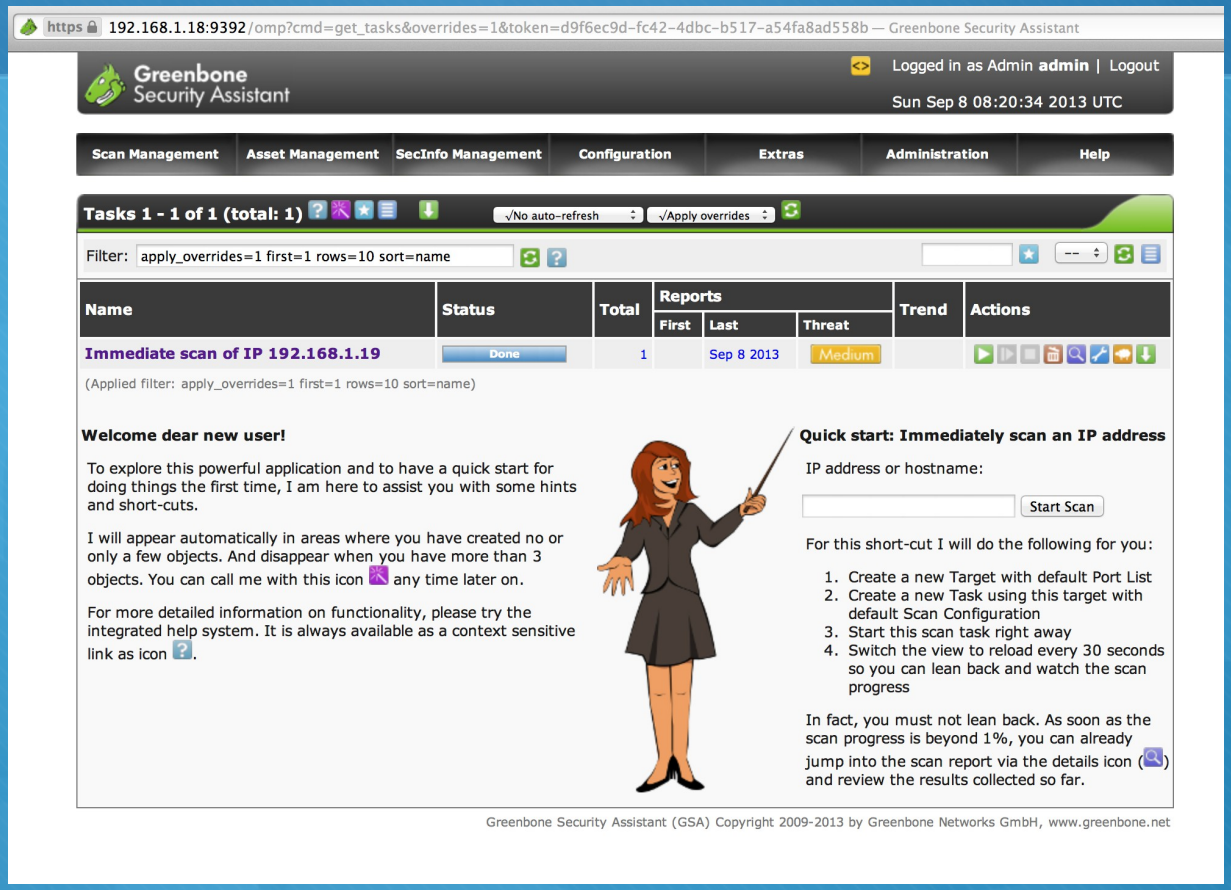
Nessus: informe de resultados



JUNTA DE ANDALUCIA

CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Openvas



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://www.slideshare.net/jmorenol/sad-tema1-introduccionii1213