

Análisis de vulnerabilidades



Análisis de vulnerabilidades

- 1. Introducción**
- 2. Proceso de inspección**
 1. Ámbito y tipos
- 3. Conceptos sobre exploits**
- 4. Aplicaciones para el análisis de vulnerabilidades**
 1. Nessus
 2. Reporting nessus
- 5. OpenVas**
- 6. Nexpose & Retina**
- 7. Análisis de vulnerabilidades**
 1. Conceptos
- 8. BBDD de vulnerabilidades**

Análisis de vulnerabilidades

Introducción

- **Se define vulnerabilidad como:**
 - *Vulnerabilidad es un fallo en el código o en la configuración de un software o en el diseño e implementación de un sistema hardware o físico, que permite a un operario comprometer la seguridad del activo y hacer que muestre y realice funciones anti producentes y para el que no está autorizado.*

Análisis de vulnerabilidades

Introducción

- Pero no sólo tiene que ser un fallo, en muchas otras ocasiones, se puede dar el caso de que el software no está diseñado pensando en muchos aspectos de seguridad. En este caso no es un fallo, sino que es una opción no contemplada. En esta situación y pese que no hay error en el diseño de la aplicación, sigue existiendo la vulnerabilidad.
- Las vulnerabilidades, de ser explotadas, pueden permitir el control total de activo y causar acciones no autorizadas contra todos los usuarios legítimos.

Análisis de vulnerabilidades

Proceso de inspección

- **Una vez estamos situados con respecto a los objetivos dentro de la auditoria y tenemos la visibilidad necesaria, vamos a ver los requisitos mínimos a la hora de empezar con la inspección de vulnerabilidades:**
 - 1.- **Tener información crítica acerca del objetivo.** En esta fase recolectaremos los datos que nos permitirán determinar los puntos débiles del activo para focalizar las entradas, **POSIBLEMENTE vulnerables**, por ejemplo, **puertos** abiertos, **software** detrás de los mismos, procesos de un sistema, etc. Este punto lo hemos cubierto en los módulos anteriores.

Análisis de vulnerabilidades

Proceso de inspección

2.- Tener información de fallos de seguridad CONOCIDOS para dirigir las vulnerabilidades. Aquí es donde debemos realizar un **proceso de investigación, y con toda la información recolectada en el punto anterior, determinar los puntos críticos del objetivo** a los que deseamos dirigir nuestro esfuerzo y adquirir información del software/versión que se está ejecutando.

Hay que **tener en cuenta que hay muchos profesionales dedicándose de forma intensiva a descubrir vulnerabilidades, algunas las notifican, otras las liberan y otras las venden, pero más tarde o más temprano, *siempre hay un momento que suelen ser de dominio público.***

Análisis de vulnerabilidades

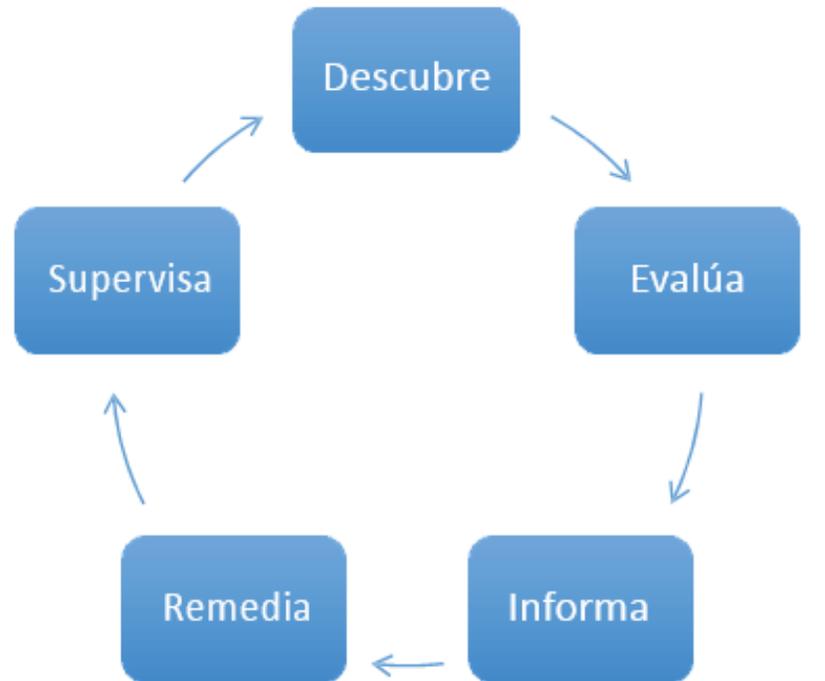
Proceso de inspección

3.- Crear el código que ponga en evidencia la vulnerabilidad y la explote. Que no exista una vulnerabilidad conocida para un proceso o software **no quiere decir que no la tenga, solamente que aún no se ha descubierto** o está en fase de investigación. **Siempre podemos diseñar nuestro propio código y explotarla nosotros,** aunque para realizar esta tarea hace falta una formación y unos **conocimientos muy elevados y concretos.**

Análisis de vulnerabilidades

Proceso de inspección - Ámbito

- El proceso a seguir desde el punto de vista de un profesional, lógico y secuencial se basa en la siguiente imagen:



Análisis de vulnerabilidades

Proceso de inspección - Ámbito

- **Descubrir:** inspeccionar un Sistema para identificar vulnerabilidades.
- **Evaluar:** principalmente el impacto de las mismas en caso de descubrirlas.
- **Informa:** establece el nivel de riesgo del activo, analiza el nivel de probabilidad de que el ataque se lleve a cabo con éxito, y genera los correspondientes informes técnicos para la documentación de la auditoría.
- **Remedia:** se genera una política o aplicación de solución para remediar las vulnerabilidades encontradas.
- **Supervisa:** periódicamente se revisa la salvaguarda de la vulnerabilidad y el correcto funcionamiento de las medidas, así como nuevas vulnerabilidades que pueden haber aparecido.

Análisis de vulnerabilidades

Proceso de inspección - Ámbito

- **En este punto deberíamos saber dónde atacar al objetivo por lo que pasaremos a buscar las brechas, pero hay que ser consciente de que el proceso puede llegar a ser muy tedioso por dos razones:**
 - **en ocasiones, son tantos los puntos de posible ataque y la cantidad de vulnerabilidades que se descubren, que es casi imposible gestionarlo todo, por ello haremos uso de bases de datos internacionales, donde se recolectan las últimas vulnerabilidades encontradas.**
 - **Otras veces aunque tengamos puntos de “entrada” es probable que no existan vulnerabilidades y exasperemos en el intento.**

Análisis de vulnerabilidades

Proceso de inspección - Ámbito

- Existen muchas bases de datos de este tipo, de las más conocidas son:
 - NVD <https://nvd.nist.gov/>
 - OSVDB <https://blog.osvdb.org/category/vulnerability-databases/>
 - SecurityFocus <http://www.securityfocus.com/>
 - PacketStorm <https://packetstormsecurity.com/>

Análisis de vulnerabilidades

Proceso de inspección - Ámbito

- Ahora nos surge un nuevo problema, **estas bases de datos son tan amplias y en muchas de ellas, los recursos que nos proveen son tan subjetivos que la aplicación de las vulnerabilidades encontradas a nuestro entorno de evaluación sería otra tarea casi "titánica"**, por este motivo ha desarrollado software que almacena gran parte de todas estas bases de datos y otras vulnerabilidades de los propios investigadores.
- Este tipo de software provee de múltiples funcionalidades. **Indicándole el objetivo lanzará todas las vulnerabilidades hacia el mismo** y según los frentes abiertos nos mostrará cuales podrían ser efectivas y detalles de las mismas.

Análisis de vulnerabilidades

Proceso de inspección – Tipos de vulnerabilidades

- Hemos visto los conceptos sobre vulnerabilidades, y dónde se pueden encontrar las bases de datos que las albergan y aglutinan. También sabemos que existe software específico que actualiza y utiliza estas bases de datos. Este software se clasifica según el ámbito del objetivo, veamos los **dos tipos de objetivos que podemos encontrarnos**.

Análisis de vulnerabilidades

Proceso de inspección – Tipos de vulnerabilidades

- Vulnerabilidades de hosts: en este grupo entran todas aquellas que hacen referencia a **ataques a los puertos de los hosts y a los servicios que están levantados** tras ellos, según el software que los lanza y su versión.
- Vulnerabilidades web: debido a la cantidad y diversificación del software que se publica en los **servidores web**, cada día proliferan más las **vulnerabilidades que intentan explotar las fallas en los mismos**, como por ejemplo errores en el código, en el manejo de cookies, configuración con deficiencias de los servidores etc...

Análisis de vulnerabilidades

Proceso de inspección – Tipos de vulnerabilidades

- Hay que tener en cuenta que **muchas vulnerabilidades son comunes entre los dos grupos.**
- Fijaros que **un servidor web no es más que un puerto o varios puertos con servicios detrás que levantan procesos**, por lo tanto estaría categorizado en **vulnerabilidades de host**, pero el ataque directo a las funcionalidades y configuraciones de estos servicios, en su lado público y las vulnerabilidades sobre el código y los protocolos de comunicación e interrelación, es de los que se encarga el grupo **de vulnerabilidades web.**

Análisis de vulnerabilidades

Conceptos sobre Exploits

- La siguiente cuestión lógica se basa en responder cómo se encarga el software de averiguar **si la vulnerabilidad es factible de explotación o no**, con la intención de verificar que la vulnerabilidad que está catalogada es explotable en nuestros sistemas objetivos, **para ello se utilizan los exploits**.

Exploit {del inglés to exploit, explotar o aprovechar} es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico

Análisis de vulnerabilidades

Conceptos sobre Exploits

- Tenemos que tener claro que **un exploit no es una vulnerabilidad**. Es el **código que explota la vulnerabilidad**, pero se puede dar el caso de que la vulnerabilidad sea explotable **sin necesidad de ningún exploit**, tan solo con cambiar o agregar algunas letras, como es el caso de muchas de las vulnerabilidades web.
- El **software especializado dispone, a parte de la base de datos de vulnerabilidades, de una relación de exploits que se lanzan**. De ese modo se determina que la misma es efectiva y se puede utilizar en ese objetivo en concreto.

Análisis de vulnerabilidades

Conceptos sobre Exploits

- Hay que dejar claro que la utilización de exploit para obtener acceso al objetivo, por ejemplo, **es otra fase de la auditoria**, pues ya obtendríamos la finalidad del ataque o al menos, iniciada.
- **En la fase de análisis de vulnerabilidades el software gestor lo utilizará para poner en evidencia la vulnerabilidad NO PARA EXPLOTARLA**, que por otro lado sería imprudente, ya que este proceso es totalmente recomendable que esté supervisado por el auditor.

Análisis de vulnerabilidades

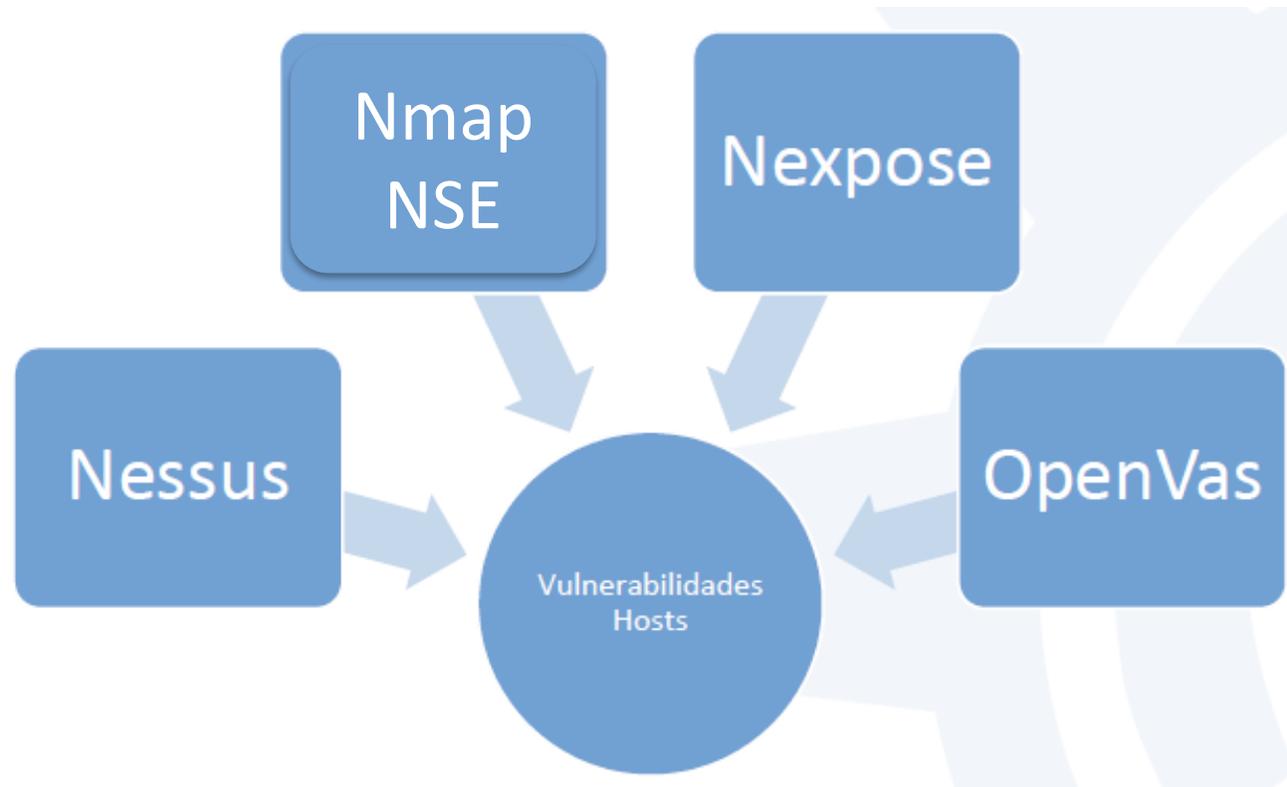
Conceptos sobre Exploits

- **Algunas bases de datos públicas de exploits son:**
 - Exploit-db <https://www.exploit-db.com/>
 - Inj3ct0r (0day) <http://es.0day.today/>
 - PacketStorm <https://packetstormsecurity.com/files/tags/exploit>
 - CxSecurity <https://cxsecurity.com/exploit/>

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades

- Software que se podría utilizar para realizar nuestras evaluaciones



Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NESSUS

- Uno de los más conocidos e importante es **Nessus**. Dispone de un **potente motor de escaneo y una base de vulnerabilidades y exploits, quizás, de las mejores existentes**. Hace un par de años contábamos con una versión para realizar análisis en un entorno particular denominada "Home", la cual tenía limitadas varias opciones (ya no está disponible), y para entornos profesionales, **disponemos de la versión “proffesional”** (pago – sobre 2.700€/año).

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NESSUS

- En una secuencia lógica, tanto Nessus como cualquier escáner de vulnerabilidades necesitará de, como mínimo, un **escaner de puertos y de servicios. Nessus puede hacer uso tanto de nmap como de un motor interno que incluye para escanear puertos.**
- **Acto seguido comenzará la carga de exploits para intentar determinar las vulnerabilidades disponibles, y por último se hará uso del lenguaje interno de scripts de Nessus NASL (Nessus Attack Scripting Language)** para determinar si hay algún script interno cargado o alguno programado por nosotros mismos, que analice las vulnerabilidades y muestre el fallo de seguridad.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

INSTALACIÓN

- Lo primero es descargar el software para kali.
- Para ello descargaremos la versión de Linux en la siguiente dirección: <http://www.tenable.com/products/nessus/select-your-operating-system> Y ejecutamos el siguiente comando:

```
#dpkg -i <nombre del paquete>
```
- A continuación iniciamos el servicio:

```
#/etc/init.d/nessusd start
```
- Y vamos a la url: <https://localhost:8834>

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

INSTALACIÓN

- Introducimos las credenciales para crear la cuenta de administrador en Nessus y nos solicitará un código de activación, el cual se puede adquirir en la página del desarrollador:
- <http://www.tenable.com/>
- Una vez introducido el código, se procederá al registro y deberemos de descargar los plugins, este proceso **puede durar varios minutos, por favor paciencia, según los recursos del sistema donde lo estéis instalando puede llegar a ser muy largo.**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

INSTALACIÓN



The screenshot shows the Nessus vulnerability scanner interface during the registration phase. At the top left is the Nessus logo with the text "Nessus vulnerability scanner". Below the logo, the heading "Registering..." is displayed in a large, bold, teal font. Underneath, a message states: "Successfully registered the scanner with Tenable. Successfully created the user." At the bottom of the registration area, there is a button with the text "Next: Download plugins >".



The screenshot shows the Nessus vulnerability scanner interface during the plugin download phase. At the top left is the Nessus logo with the text "Nessus vulnerability scanner". Below the logo, the heading "Nessus is fetching the newest plugin set" is displayed in a large, bold, teal font. To the right of this heading, the text "Please wait..." is shown. Below the heading and text, there is a progress bar consisting of a teal segment followed by a grey segment. At the bottom of the screen, a message states: "The Nessus server is now downloading the newest plugins from Tenable which may tak".

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

INSTALACIÓN

- Durante el proceso de descarga se obtendrán todos los **ficheros nasl**, que contienen las evaluaciones de seguridad que luego se lanzarán.
- Seguirá con el proceso de inicialización, mediante el cual cargará los plugins en el software y realizará las configuraciones básicas, **otro proceso que puede llegar a tardar un rato**.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN

- Abrimos la dirección url de Nessus e indicamos las credenciales definidas con anterioridad y una nueva página aparecerá en nuestro navegador, donde **comenzaremos a interrelacionar con el sistema de gestión de análisis de vulnerabilidades.**
- Nos encontramos ante el panel de administración del software. A continuación vamos a situarnos en la última pestaña, "Users", aquí podrás gestionar los usuarios existentes o dar de alta y nuevos.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN



The screenshot shows the Nessus web interface for user management. The top navigation bar includes the Nessus logo and links for Scans, Schedules, Policies, and Users. The main content area is titled 'Users' and features a search bar. A 'New User' button is visible on the left. The 'All Users' section displays a table with the following data:

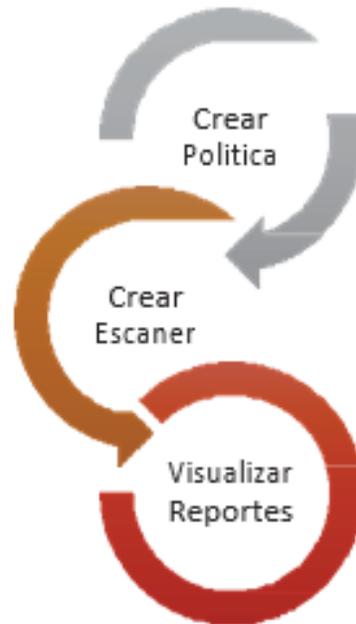
<input type="checkbox"/>	Name ▼	Last Login	Type
<input type="checkbox"/>	admin	May 16, 2014 13:59:53	Administrator

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN

- Vamos a ver el proceso que deberemos seguir para configurar una secuencia de escaneo personalizada:

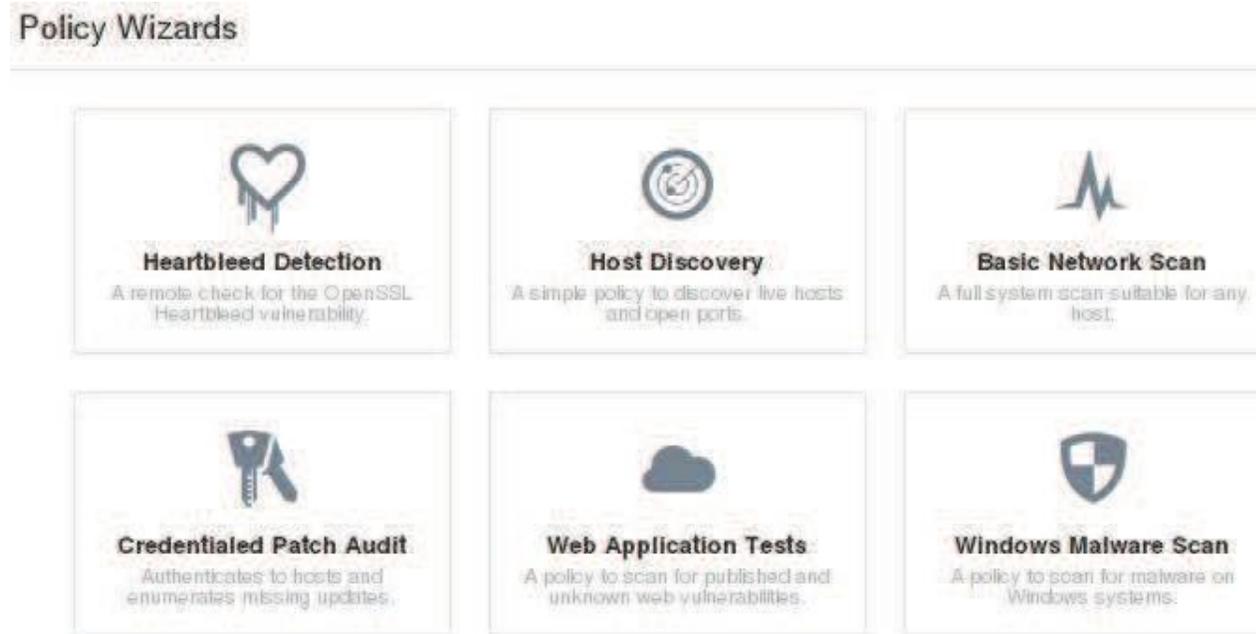


Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN – Crear política

- Nos situamos en la sección de "Políticas" y pulsamos sobre "New Policy", veremos cómo nos aparece una pantalla similar a la siguiente:



Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NESSUS

UTILIZACIÓN – Crear política

- Aquí podremos **seleccionar patrones de análisis y preconfiguraciones** establecidas para realizar inspecciones bajo aspectos concretos, por ejemplo, disponemos Heartbleed Detection donde escaneará la red e identificará la vulnerabilidad sobre OpenSSL, y nos notificará sobre ello.
- **Por ejemplo "Basic Network Scan", cubriría todas las necesidades de inspección sobre los dispositivos de la infraestructura para el ejemplo de crear una política.**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN – Crear política

- Introducimos el **nombre de política y la visibilidad**, esta sirve para que otros usuarios puedan utilizarla dentro de sus entornos.

New Basic Network Scan Policy / Step 1 of 3

1 Define your policy name, description, visibility, and post-scan editing preferences:

Policy Name	<input type="text" value="Test_1"/>
Visibility	<input type="text" value="private"/>
Description	<input type="text" value="brief description of the policy goes here"/>
Allow Post-Scan Report Editing	<input checked="" type="checkbox"/>

New Basic Network Scan Policy / Step 2 of 3

2 Choose the type of scan to configure:

Scan type	<input type="text" value="Internal"/>
-----------	---------------------------------------

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN – Crear política – credentials

- El sistema de autenticación **se establece para poder aplicar los análisis directamente en zonas solamente accesibles a través de una previa autenticación.**
- En una auditoría es común haber extraído algún tipo de clave de usuario, a través de métodos de interceptación del hash y descifrado, o inyectando directamente y se podría usar.
- Una vez terminada la configuración **la guardamos con "Save" y la podremos usar sucesivas veces.**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NESSUS

UTILIZACIÓN – Crear política – Modo avanzado

- Lo activaremos en el menú de la izquierda, "Advanced".
- Aquí podremos **configurar los parámetros más importantes para que ayude al consultor a determinar de forma rápida las mejores opciones y configuraciones según el tipo de escaneo.**
- La política podrá usarse posteriormente como un perfil de escaneado personalizado.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades - NISSUS

UTILIZACIÓN – Lanzando escaneo básico rápido

- 1.- Seleccionamos “New Scan”
- 2.- Escogemos la plantilla “Basic Network Scan”
- 3.- Completamos los campos que se nos indican y añadimos los hosts (Ips). También podríamos subir un archivo con las ips.
- 4.- Guardamos el “scan” con “save”.
- 5.- Nos vamos al menú superior Scans y en el listado que aparece, para lanzar el escaneo, pulsamos el botón del “play” (triángulo a la derecha de la línea del escaneo). Se inicia el proceso.

Análisis de vulnerabilidades - Práctica

Aplicaciones para el análisis de vulnerabilidades – NISSUS

- Generar una nueva política de escaneo para que esté disponible en el repositorio de Nessus
- Realizar un escaneo básico sobre un equipo o la red actual.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Reportes NESSUS

- Qué sucedería si estamos trabajando en un equipo donde solamente nos interesa ver los reportes que han generados otros compañeros, o tenemos varios equipos y usuarios con roles diferentes y para algunos de ellos sólo nos interesa tener privilegios para que solamente puedan acceder a los resultados. Para ello hay una herramienta llamada "**Nessie Viewer**".
- Desde Nessus podemos exportar los resultados de nuestros análisis a ficheros con extensión **.nessus**.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Reportes NISSUS

The screenshot displays the Nessus web interface. At the top, there is a navigation bar with the Nessus logo and tabs for Scans, Schedules, Policies, and Users. The main content area shows a 'Network_Scan' report for the host '192.168.1.168'. A table lists vulnerabilities, with the first one being 'CRITICAL' and 'PHP Unsupported Version Detection'. A modal dialog is open in the foreground, titled 'Opening nessus_report_Network_Scan.nessus'. The dialog text reads: 'You have chosen to open: nessus_report_Network_Scan.nessus which is: BIN file (259 KB) from: https://localhost:8834'. It asks 'Would you like to save this file?' and provides 'Cancel' and 'Save File' buttons.

Severity	Plugin Name
CRITICAL	PHP Unsupported Version Detection
HIGH	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	PHP 5.2 < 5.2.14 Multiple Vulnerabilities

Opening `nessus_report_Network_Scan.nessus`

You have chosen to open:

- `nessus_report_Network_Scan.nessus`
which is: BIN file (259 KB)
from: `https://localhost:8834`

Would you like to save this file?

Cancel Save File

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Reportes NNESSUS

- Después abrimos **Nessie** -> **File** -> **Open Nessus Report**, y **automáticamente cargará los resultados del fichero** en un visor, donde en el panel de la izquierda podremos ver los plugins, los hosts, el puerto afectado, el servicio y el sistema operativo.
- A parte tendremos a nuestra disposición **un completo filtro**, ya que si disponemos de múltiples hosts escaneados nos será difícil localizar información crítica.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Reportes NISSUS

The screenshot displays the Nessus report interface. At the top, there is a menu bar with 'File', 'Options', 'View', and 'Generate'. Below the menu, it indicates 'Number of rows: 22/22'. The main table lists vulnerabilities with columns for ID, Plugin Name, Host IP, Port, Service, and OS. The selected row (ID 10736) is highlighted in blue. Below the table is a 'Filters' section with input fields for Host IP, Host Name, Port, Service, OS, Plugin Name, Plugin ID, Plugin Output, and Risk, along with a 'Clear Filters' button and an 'Exploit available' checkbox. To the right of the table, there is a detailed view for the selected vulnerability, including 'Host info', 'Host Name', 'Synopsis', 'Description', and a list of available DCERPC services.

ID	Plugin Name	Host IP	Port	Service	OS
10736	DCE Services Enumeration	192.168.0.22	49158	dce-rpc	Windows
10736	DCE Services Enumeration	192.168.0.22	49157	dce-rpc	Windows
10736	DCE Services Enumeration	192.168.0.22	49155	dce-rpc	Windows
10736	DCE Services Enumeration	192.168.0.22	49154	dce-rpc	Windows
10736	DCE Services Enumeration	192.168.0.22	49153	dce-rpc	Windows
10736	DCE Services Enumeration	192.168.0.22	49152	dce-rpc	Windows
10397	SMB LanMan Pipe Server Listing Discl...	192.168.0.22	445	cifs	Windows
26917	SMB Registry : Nessus Cannot Access...	192.168.0.22	445	cifs	Windows
26920	Windows SMB NULL Session Authenti...	192.168.0.22	445	cifs	Windows
10394	SMB Log In Possible	192.168.0.22	445	cifs	Windows
10785	SMR Native LanMan Remote Syst	192.168.0.22	445	cifs	Windows

Host info : 192.168.0.22:49153 (dce-rpc) - Windows 7 Ultimate
Host Name : RafaPC

DCE Services Enumeration (10736)

Synopsis
A DCE/RPC service is running on the remote host.

Description
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.0.22

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.0.22

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Reportes NNESSUS

- Otra herramienta similar a Nessie es NetworkScanViewer
- Todo el funcionamiento es muy parecido a Nessie

The screenshot displays the Nessus Network Scan Viewer interface. At the top, there are menu options: File, Tools, Help. Below the menu, there are filters for Type (Nessus), IP (192.168.0.22), Port, Service, and a Search field. The main area is divided into two panes. The left pane shows a table of scan results, and the right pane shows a detailed description of the selected result.

Type	IP Address	Host Na...	Port	Protocol	State	Service	Sei
Nessus	192.168.0.22	RafaPC	80	tcp		www	0
Nessus	192.168.0.22	RafaPC	135	tcp		epmap	0
Nessus	192.168.0.22	RafaPC	139	tcp		smb	0
Nessus	192.168.0.22	RafaPC	443	tcp		www	0
Nessus	192.168.0.22	RafaPC	445	tcp		cifs	0
Nessus	192.168.0.22	RafaPC	912	tcp		vmware_auth	0
Nessus	192.168.0.22	RafaPC	49158	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	49157	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	49155	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	49154	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	49153	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	49152	tcp		dce-rpc	1
Nessus	192.168.0.22	RafaPC	445	tcp		cifs	1
Nessus	192.168.0.22	RafaPC	445	tcp		cifs	1
Nessus	192.168.0.22	RafaPC	445	tcp		cifs	1
Nessus	192.168.0.22	RafaPC	445	tcp		cifs	1

Description: It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Synopsis: Nessus is not able to access the remote Windows Registry.

Plugin Version: \$Revision: 1.7 \$
Risk Factor: None
Plugin Publication Date: 2007/10/04
Plugin Output:
Could not connect to the registry because:
Could not connect to \winreg

Loaded 28 results

Análisis de vulnerabilidades - Práctica

Aplicaciones para el análisis de vulnerabilidades – Reportes NISSUS

- De los escaneos realizados en la práctica anterior, exporta desde nessus el archivo correspondiente y ábrelo con las aplicaciones comentadas.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Existe una máquina virtual especialmente diseñada para el análisis de vulnerabilidades y que se integra con Nessus, se llama Vsam (<http://vsam.sourceforge.net/>).
- Entre las características que nos ofrece:
 - Completa integración con Nessus
 - Copia de seguridad y restauración
 - Las copias de seguridad se pueden descargar
 - Escaneos programados o manuales
 - Seguimiento de hosts y solución
 - Cálculo de métrica y de tendencias
 - Búsquedas completas y un largo etcétera

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Tras descargarla en nuestro equipo la abrimos con VMWare (No Vbox).
- Arrancará una máquina virtual llamada "Vsam Production"
- Ahora vamos a continuar lanzando el script de configuración que nos permitirá interactuar con la máquina virtual.
- Primero entramos en la shell a través de la pantalla de la máquina virtual, con las credenciales User = root Pass = password e introducimos:
`./setup`

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Automáticamente se lanzará la configuración, y empezamos a introducir información:

```
Vsam installation setup script
Please fill in all required information. This script will then configure the ap
pliance for use

Setup IP Configuration
Please note that the appliance will require access to Internet in order to downl
oad plugin updates.
Please ensure that access to the nessus update site is available.

Appliance interface to use. Setup has auto-detected the following available Inte
rface
eth3

If the interface above is ok then hit enter to select, otherwise enter another i
nterface to use
-
```

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Lo primero que **debemos introducir es la ip que va a tener la máquina virtual (Bridge)**, y a partir de aquí comenzará una serie de preguntas, todas referentes a los datos técnicos, y sencillas de rellenar, tan sólo hay que introducir, en un momento, **la clave de registro de la página de Nessus.**
- Ahora desde un ordenador **en la misma red**, accedemos al navegador e introducimos `https://ipmaquinavirtual`

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Veremos cómo se abre una pantalla que nos solicita credenciales, en este punto deberemos introducir: User = admin Pass = password
- Nos aparecerá una pantalla similar a la siguiente:

The screenshot displays the Vsam Vulnerability Management interface. At the top left is the Vsam logo. A navigation menu includes Home, Dashboard, Settings, Security Scan, Reports, Search, Infrastructure, Maintenance, and Logout. The main content area is divided into two columns. The left column contains 'My Totals' (Scanned 0 systems, 0 times) and 'Pending Exceptions' (There are 0 exceptions in the database). The right column contains 'System Stats' with 'Plugin Count' (38413 plugins in the database, 0 new added in last 7 days) and 'Scan Queue' (0 scans running or queued). A table header for pending exceptions is visible at the bottom left of the main area.

Vsam v1.10
Logged in as: admin
System Time: 02/25/2011 19:30:20
Timezone: America/New_York

Home Dashboard Settings Security Scan Reports Search Infrastructure Maintenance Logout

My Totals
Scanned 0 systems, 0 times.

System Stats

Plugin Count:
There are 38413 Nessus plugins in the database.
0 new plugins added within last 7 days.

Scan Queue:

You have:
0 Nessus scans currently running.
0 Nessus scans currently queued for scanning.

InProtect has:
0 Nessus scans currently running.
0 Nessus scans currently queued for scanning.

Pending Exceptions
There are 0 exceptions in the database.

Latest 0 pending exceptions

EID	IP	SubmitDate	plugin type
-----	----	------------	-------------

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Vsam

- En este punto ya tenemos Nessus en nuestra máquina virtual a pleno rendimiento **con muchas más funciones.**
- Si deseamos indicar que el servidor de Nessus se encuentra en otra dirección IP, lo podemos hacer desde Setting-Nessus Server.
- **Es una aplicación con Nessus como base, por lo que todos los conceptos vistos para este son aplicables a la misma.**

Análisis de vulnerabilidades - Práctica

Aplicaciones para el análisis de vulnerabilidades – Vsam

- Trata de realizar un escaneo sobre tu red actual y considera los resultados

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- **OpenVas (Open Vulnerability Assessment System) es un fork de Nessus, es la alternativa libre del mismo**, decimos libre porque antes Nessus era de código libre, ahora desde que lo compraron Tenable el código es privado y las funcionalidades están limitadas a la versión que se compre.
- **OpenVas no sólo utiliza su base de firmas de vulnerabilidades sino que hace acopio de mucho software de terceros y sus beneficios para incrementar su funcionalidad y rendimiento. Algunos programas que usa son nmap, Amap, nikto, TripWire, Tiger, etc.**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- OpenVas antes **estaba disponible en kali**, desde la versión 2 (sana) tenemos que descargarla.
 - `root@kali:~# apt-get install openvas`
`root@kali:~# openvas-setup`
- **Se realizarán todas las tareas de preconfiguración** (introducción de credenciales, etc.) y descarga de plugins necesarios para el correcto funcionamiento del escáner.
- **Este proceso puede tardar**, debido a la carga de tareas que se realizan de forma secuencial, paciencia.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- **Cuando finalice, comprobamos que el servicio está en escucha:**

```
# netstat -antp
```

```
Active Internet connections (servers and established)
```

```
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
```

```
tcp 0 0 127.0.0.1:9390 0.0.0.0:* LISTEN 9583/openvasmd
```

```
tcp 0 0 127.0.0.1:9391 0.0.0.0:* LISTEN 9570/openvassd: Wai
```

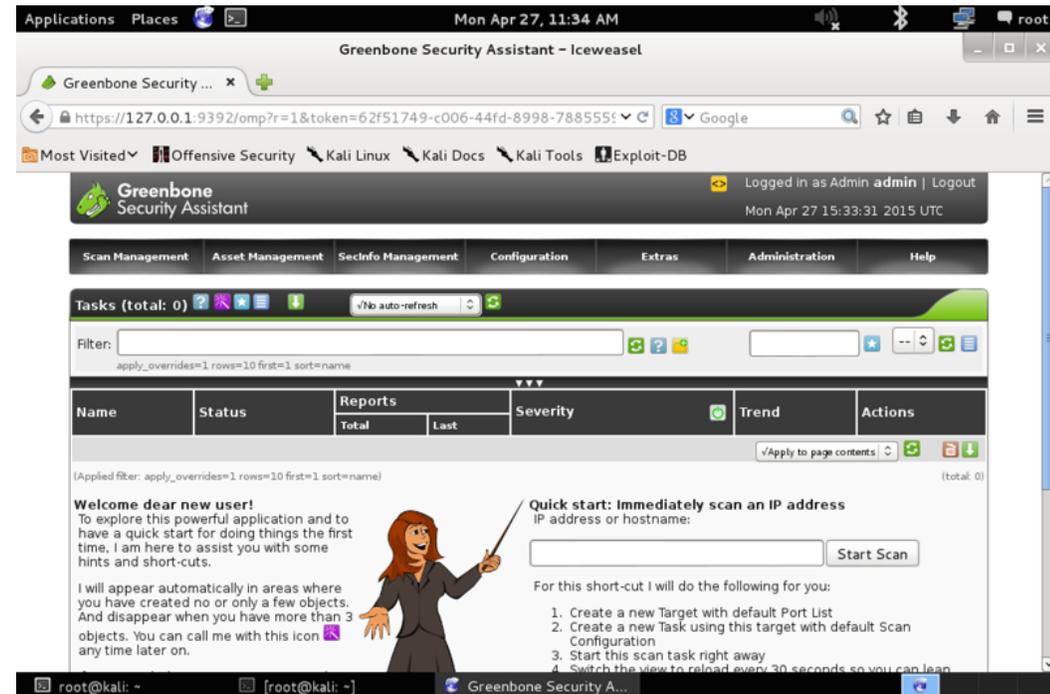
```
tcp 0 0 127.0.0.1:9392 0.0.0.0:* LISTEN 9596/gsad
```

- **A continuación iniciamos OpenVAS con el comando #openvas-start**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Para conectarnos al interfaz, simplemente tenemos que acceder a <https://127.0.0.1:9392> y aceptar el certificado.
- **NOTA:** hay que tener en cuenta que si nos encontramos tras un firewall que filtre nuestras comunicaciones no será posible la actualización de forma correcta.



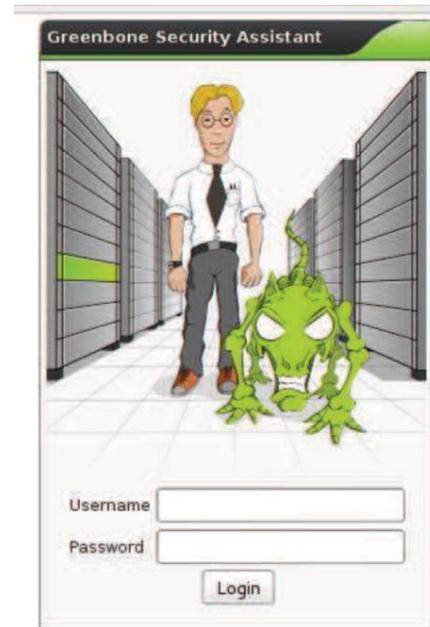
Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Problemas al arrancar: si detectamos que nos da algún fallo, el cual será significativo por la indicación a través de la palabra "ERROR", podemos intentar reiniciar el servidor, y en una gran mayoría de ocasiones se solucionará.

`sudo /etc/init.d/openvas-server start`

O desde el menú de la kali “Vulnerability...”



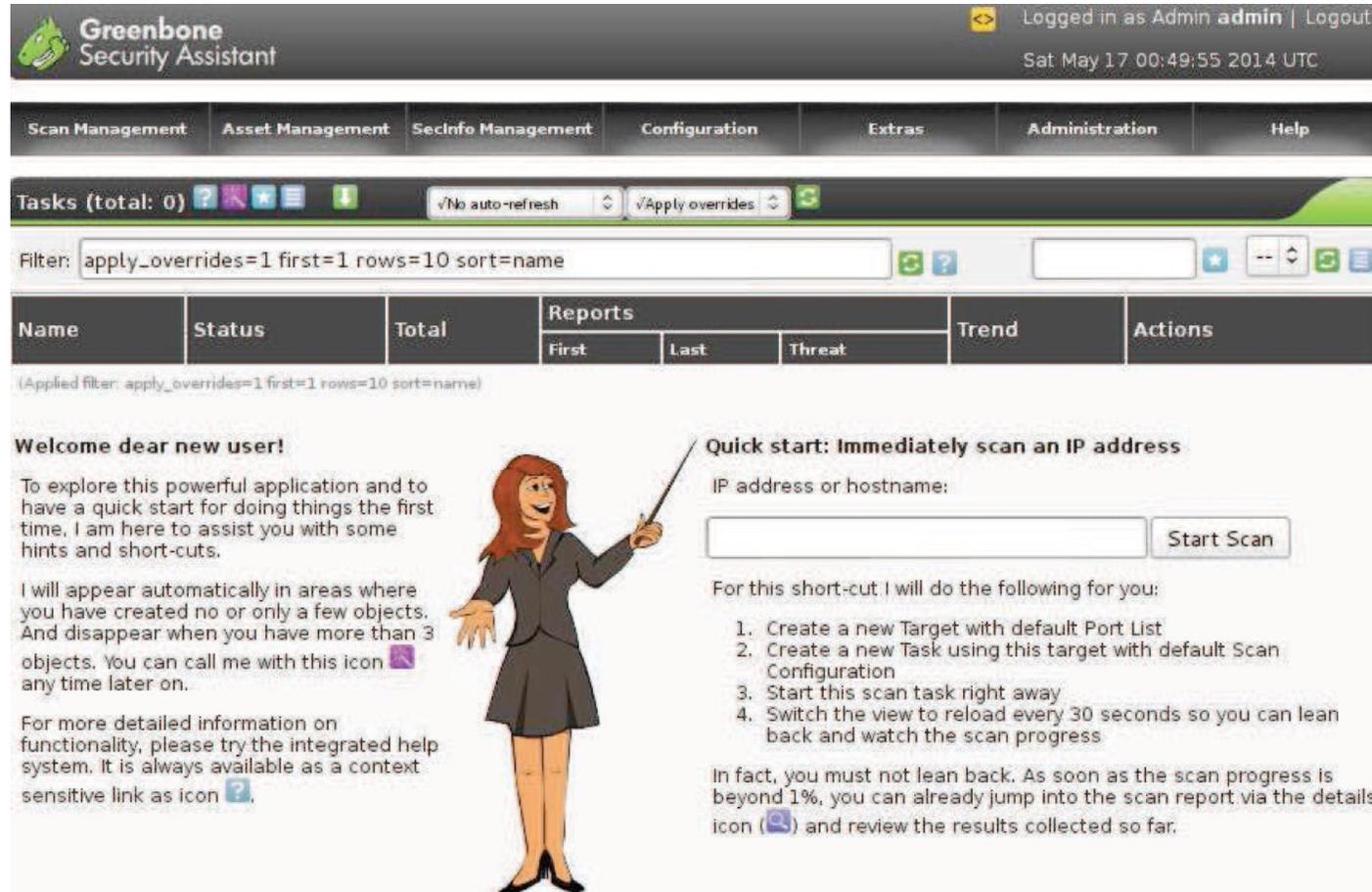
Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Al igual que Nessus, **hará falta un usuario para interactuar con OpenVas** para ello introducimos "admin" y la contraseña que hemos introducido en el proceso de inicialización.
- Ahora estamos **listos para arrancar la interfaz de configuración**, antes había un cliente específico, en la nueva versión se puede interactuar a través de web, y del cliente de Linux, nosotros continuaremos en la versión web.
- Si tenemos problemas con el usuario, modificamos la contraseña con el comando:
 - `openvasmd -user=admin --new-password=password`

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS



The screenshot displays the Greenbone Security Assistant (GSA) web interface. At the top, the logo and name 'Greenbone Security Assistant' are visible, along with the user 'Admin admin' and the date 'Sat May 17 00:49:55 2014 UTC'. A navigation bar includes 'Scan Management', 'Asset Management', 'Secinfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. Below this, a 'Tasks (total: 0)' section shows a filter: 'apply_overrides=1 first=1 rows=10 sort=name'. A table header is visible with columns: Name, Status, Total, Reports (sub-columns: First, Last, Threat), Trend, and Actions. The main content area features a 'Welcome dear new user!' message from a cartoon character, a 'Quick start: Immediately scan an IP address' section with an input field and 'Start Scan' button, and a list of actions performed by the short-cut.

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:

For this short-cut, I will do the following for you:

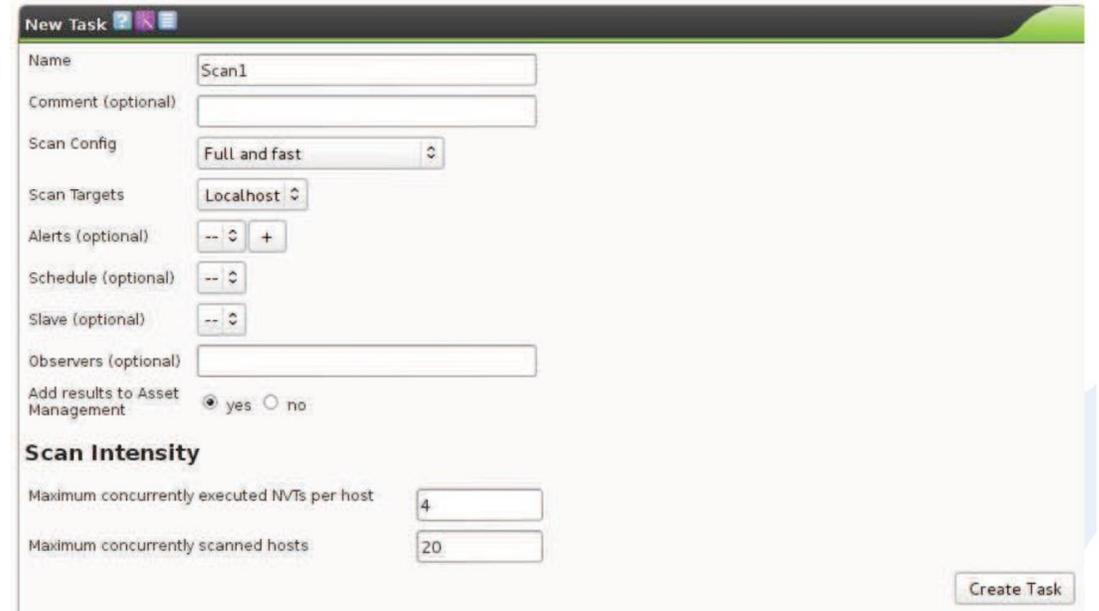
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

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.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Ahora vamos a **crear un nuevo ámbito de análisis** y una tarea nueva, para ello vamos a la siguiente menú:
 - Scan Management -> New Task
- Veremos que aparece **nuestra nueva tarea**, la cual nombraremos como deseemos, y por el momento, la dejaremos tal cual, sin configurar ninguna opción.



The screenshot shows the 'New Task' configuration window in OpenVAS. The window title is 'New Task'. The form contains the following fields and options:

- Name: Scan1
- Comment (optional):
- Scan Config: Full and fast
- Scan Targets: Localhost
- Alerts (optional): -- +
- Schedule (optional): --
- Slave (optional): --
- Observers (optional):
- Add results to Asset Management: yes no
- Scan Intensity:
 - Maximum concurrently executed NVTs per host: 4
 - Maximum concurrently scanned hosts: 20
- Create Task button

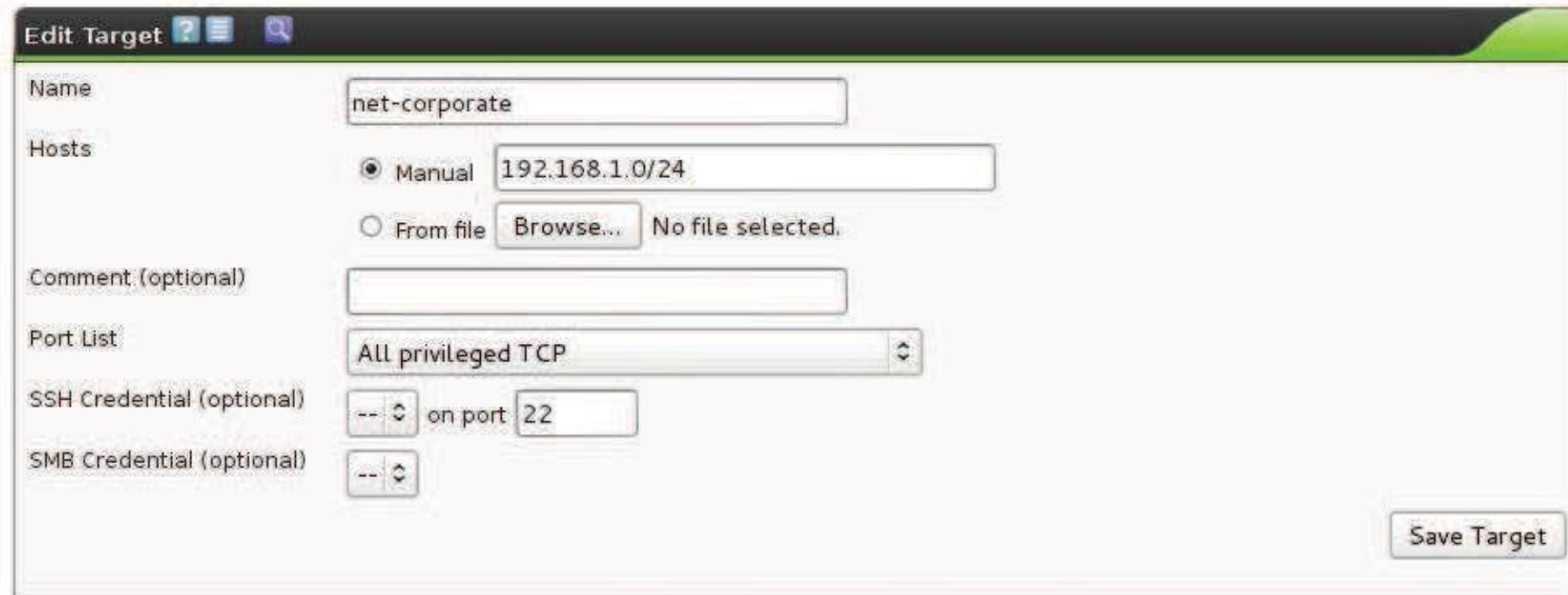
Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- **Vamos a proceder a diseñar los parámetros que se utilizarán en la configuración y optimización de la misma:**
 - **Configuration -> Port Lists** : disponemos de varios grupos predefinidos según estándares y conceptos de utilización, **en la gran mayoría de las veces será más que suficiente para realizar nuestros escáneres**, pero si deseamos generar nuestros propios grupos **lo podemos hacer pulsando sobre la estrella**, introduciendo el nombre del grupo, y el rango de puertos.
 - **Configuration -> Credentials**: al igual que hemos realizado con Nessus, **podemos especificar credenciales**, en el caso de haberlas descubierto en un proceso anterior (ingeniería social, o porque el cliente nos ha autorizado a realizar inspecciones)
 - **Configuration -> Targets**: aquí podemos crear grupos de objetivos, los cuales serán asignados a las tareas generadas, para crearlos deberemos pulsar sobre el símbolo de la estrella, a continuación introduciremos el nombre de la configuración de los objetivos, el grupo de hosts o red donde deseamos aplicar el escáner, puede ser seleccionado desde un fichero.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS



The screenshot shows the 'Edit Target' window in OpenVAS. The window title is 'Edit Target'. The form contains the following fields and options:

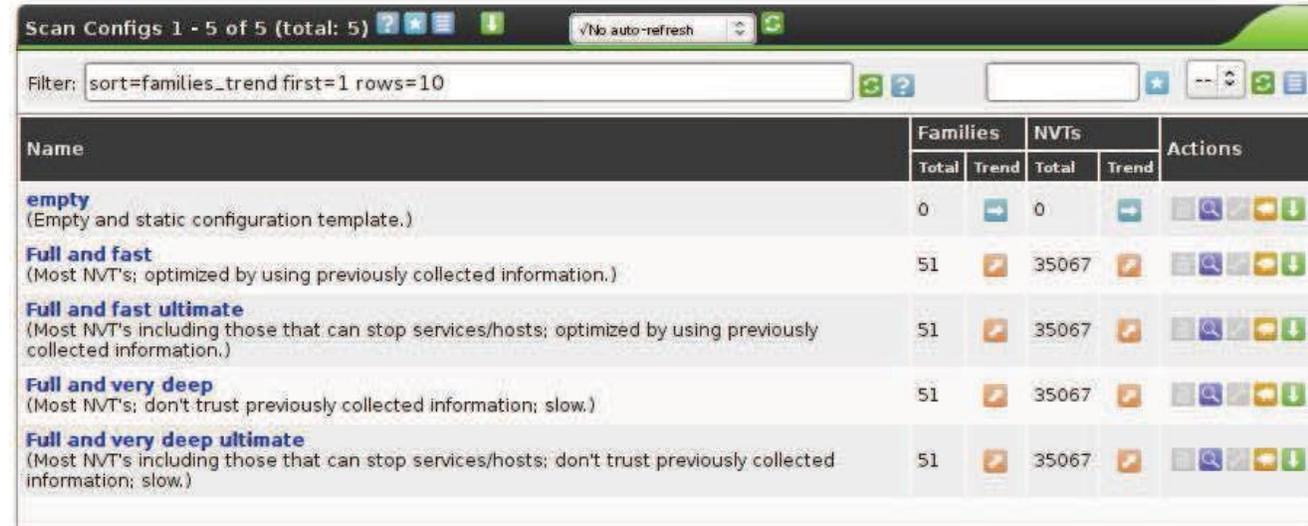
- Name:** A text input field containing 'net-corporate'.
- Hosts:** A section with two radio buttons: 'Manual' (selected) and 'From file'. The 'Manual' option has a text input field containing '192.168.1.0/24'. The 'From file' option has a 'Browse...' button and the text 'No file selected.'.
- Comment (optional):** An empty text input field.
- Port List:** A dropdown menu showing 'All privileged TCP'.
- SSH Credential (optional):** A dropdown menu showing '--' followed by 'on port' and a text input field containing '22'.
- SMB Credential (optional):** A dropdown menu showing '--'.

A 'Save Target' button is located in the bottom right corner of the window.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Ahora configuraremos los grupos de análisis de vulnerabilidades, los cuales serán aplicables a los diferentes tipos de escaneo que configuremos.
- Configuration -> Scan Configs



The screenshot shows the 'Scan Configs' interface in OpenVAS. At the top, it displays 'Scan Configs 1 - 5 of 5 (total: 5)' and a filter box containing 'sort=families_trend first=1 rows=10'. Below the filter is a table with the following data:

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
empty (Empty and static configuration template.)	0	→	0	→	🔍 🗑️ ⚙️
Full and fast (Most NVT's; optimized by using previously collected information.)	51	↗️	35067	↗️	🔍 🗑️ ⚙️
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	51	↗️	35067	↗️	🔍 🗑️ ⚙️
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	51	↗️	35067	↗️	🔍 🗑️ ⚙️
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	51	↗️	35067	↗️	🔍 🗑️ ⚙️

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Podemos observar que ya se encuentran establecidos diferentes grupos por defecto, los cuales obedecen a unas características concretas, que reflejan fielmente en el nombre que se le ha designado.
- **Características a tener en cuenta:**
 - **Families:** indican todas aquellas familias de plugins que se encuentran dentro del grupo, una familia puede ser, por ejemplo "Databases", la cual designará a las vulnerabilidades relacionadas con bases de datos
 - **Trend:** las diferentes familias, según nuevas actualizaciones, es posible que se amplíen o modifiquen, en este apartado podemos configurar su modo de actualización, la flecha azul indica "Actualización Estática", es decir no se modificarán cuando se actualice la base de firmas .

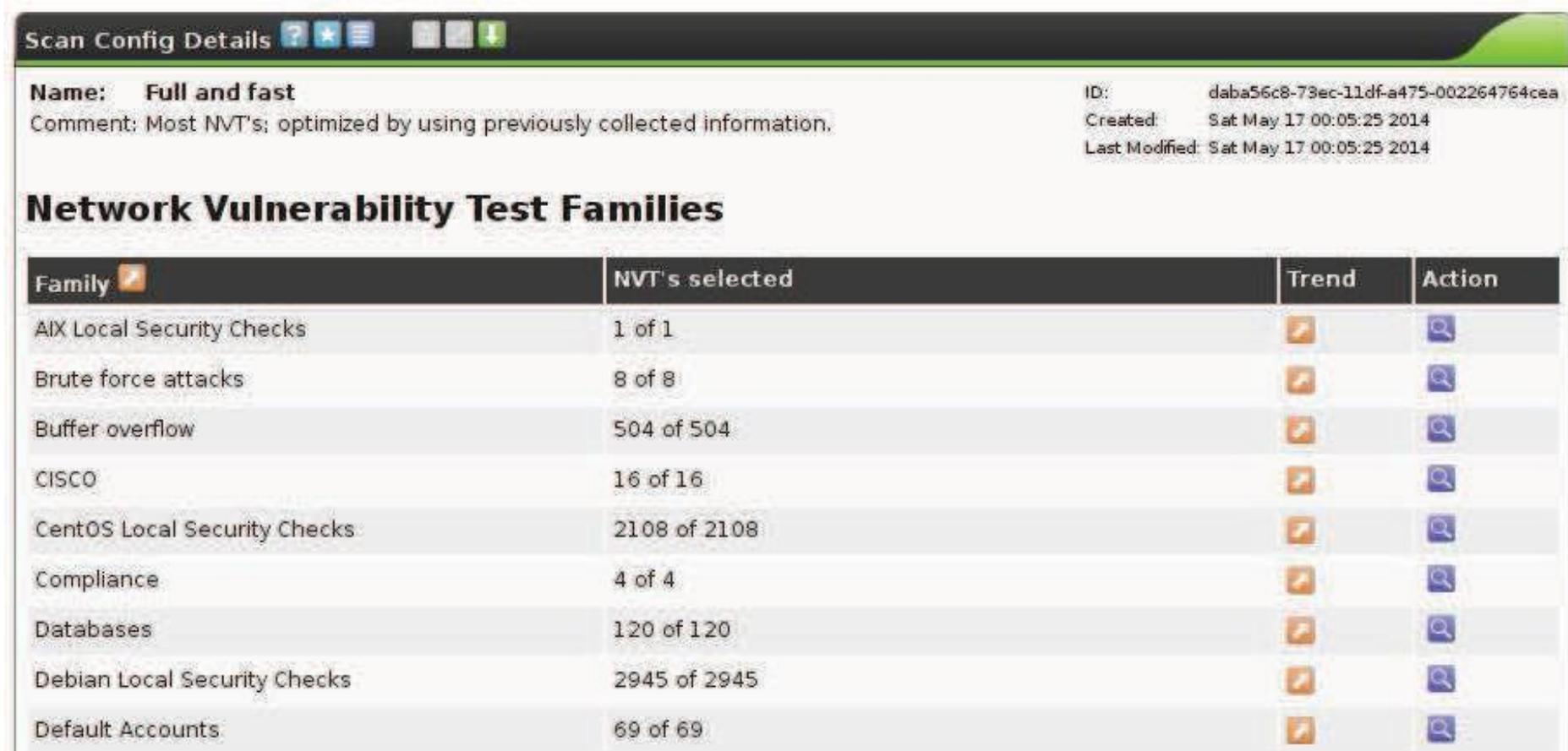
Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- **NVT,s:** hace referencia a las vulnerabilidades concretas que son contenidas dentro de las familias, las cuales están catalogadas en múltiples repositorios públicos que OpenVAS se encarga de consultar y añadir, actualmente se encuentran alrededor de las 35.000 vulnerabilidades conocidas
 - **Total:** el número de vulnerabilidades totalizadas, las cuales se encuentran clasificadas por las diferentes familias.
 - **Trend:** al igual que pasaba con las familias, la actualización de las vulnerabilidades puede ser automática o manual, quedando los repositorios fijos o dinámicos, ambos estados se controlarán con las flechas azules, estáticos, o dinámicos, naranjas.
- **Actions:** aquí podremos realizar las diferentes acciones sobre los grupo creados, como por ejemplo clonar, ver, editar, exportar, etc.
- Si editamos o vemos un grupo de vulnerabilidades podemos observar, con más detalle su contenido.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS



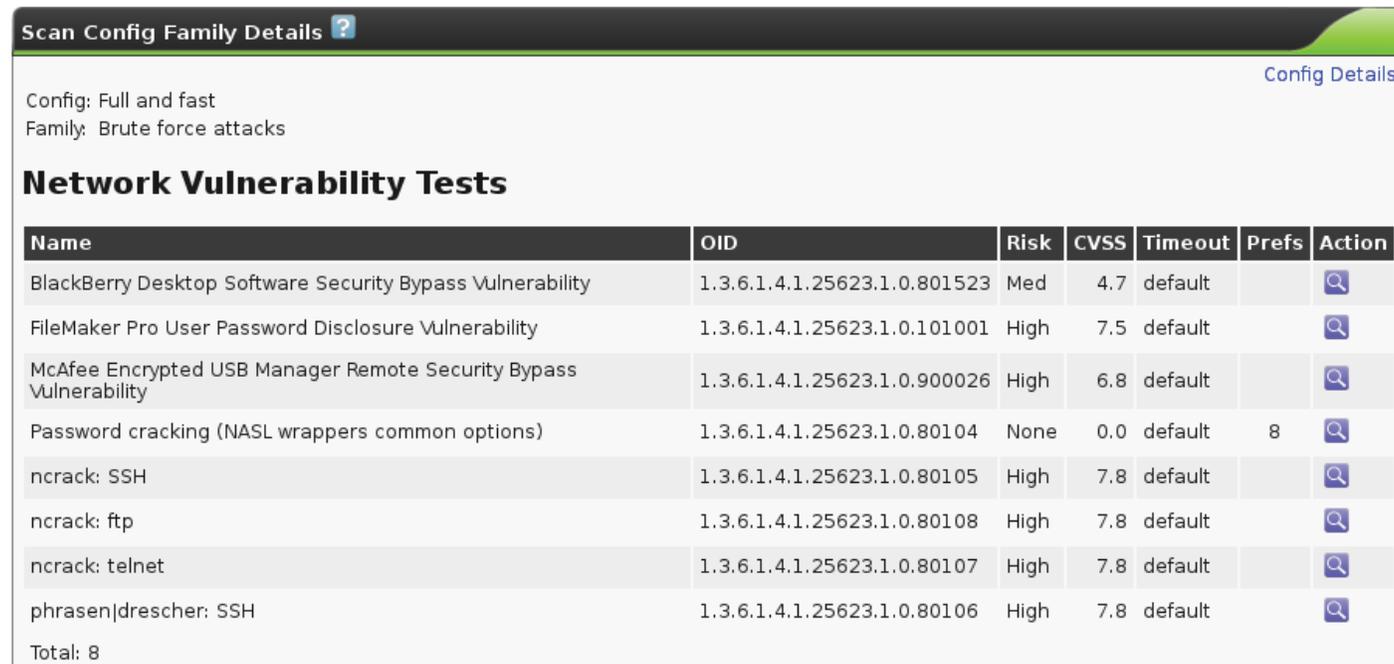
The screenshot shows the 'Scan Config Details' page in OpenVAS. At the top, there are navigation icons for help, home, and search. Below the title bar, the configuration name is 'Full and fast' with a comment: 'Most NVT's; optimized by using previously collected information.' The ID is 'daba56c8-73ec-11df-a475-002264764cea', created on 'Sat May 17 00:05:25 2014', and last modified on the same date. The main section is titled 'Network Vulnerability Test Families' and contains a table with columns for Family, NVT's selected, Trend, and Action.

Family	NVT's selected	Trend	Action
AIX Local Security Checks	1 of 1		
Brute force attacks	8 of 8		
Buffer overflow	504 of 504		
CISCO	16 of 16		
CentOS Local Security Checks	2108 of 2108		
Compliance	4 of 4		
Databases	120 of 120		
Debian Local Security Checks	2945 of 2945		
Default Accounts	69 of 69		

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Si a su vez visualizamos una familia podremos ver las vulnerabilidades que la compone, las cuales serán ejecutadas y evaluadas en un objetivo.



Scan Config Family Details [?](#) [Config Details](#)

Config: Full and fast
Family: Brute force attacks

Network Vulnerability Tests

Name	OID	Risk	CVSS	Timeout	Prefs	Action
BlackBerry Desktop Software Security Bypass Vulnerability	1.3.6.1.4.1.25623.1.0.801523	Med	4.7	default		
FileMaker Pro User Password Disclosure Vulnerability	1.3.6.1.4.1.25623.1.0.101001	High	7.5	default		
McAfee Encrypted USB Manager Remote Security Bypass Vulnerability	1.3.6.1.4.1.25623.1.0.900026	High	6.8	default		
Password cracking (NASL wrappers common options)	1.3.6.1.4.1.25623.1.0.80104	None	0.0	default	8	
ncrack: SSH	1.3.6.1.4.1.25623.1.0.80105	High	7.8	default		
ncrack: ftp	1.3.6.1.4.1.25623.1.0.80108	High	7.8	default		
ncrack: telnet	1.3.6.1.4.1.25623.1.0.80107	High	7.8	default		
phrasen drescher: SSH	1.3.6.1.4.1.25623.1.0.80106	High	7.8	default		

Total: 8

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- **Configuration -> Alerts:** en este apartado podremos indicar sucesos específicos que se llevarán a cabo bajo eventos específicos.
 - Por ejemplo, cuando termine un escaneo se podría enviar un email con un reporte del mismo al administrador, y se agregará una entrada en el syslog.
- **Configuration -> Schedule:** en este apartado diseñaremos la periodicidad y temporalidad de nuestros análisis.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Administration -> NVT Feed, SCAP Feed , CERT Feed
 - Es imprescindible actualizar las tres Fuentes de vulnerabilidades de las que se nutre OpenVAS, para disponer de toda la potencia, y las principales brechas actuales sobre sistemas y software.

SCAP Feed Management ?

Name	OpenVAS SCAP Feed
Feed Version	201405210716
Description	Synchronization in progress . Started Sat May 24 08:18:52 2014 by admin . This script synchronizes a SCAP collection with the 'OpenVAS SCAP Feed'. The 'OpenVAS SCAP Feed' is provided by 'The OpenVAS Project'. Online information about this feed: 'http://www.openvas.org/'.

Synchronize with SCAP Feed now

[Learn about the side effects of SCAP Feed synchronization!](#)

New Schedule ?

Name	<input type="text" value="unnamed"/>
Comment (optional)	<input type="text"/>
First Time	<input type="text" value="06"/> h <input type="text" value="30"/> , <input type="text" value="24"/> <input type="text" value="May"/> <input type="text" value="2014"/>
Period (optional)	<input type="text" value="0"/> hour(s)
Duration (optional)	<input type="text" value="0"/> hour(s)

Create Schedule

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

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

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- Ya nos encontramos en **disposición de terminar de configurar nuestra tarea, la cual dejamos generada, pero sin terminar de completar.**
- Editamos la tarea primaria, **Scan Management -> Task**, editamos, y **comenzamos a completar los campos con los parámetros apropiados, los cuales hemos ido creando en los apartados anteriores.**
- **Finalmente ejecutamos la tarea** para que comience la inspección de vulnerabilidades en el rango definido.
- Nomenclatura
 - NVT -> Network vulnerability tests.
 - NASL -> Nessus Attack Scripting Language.

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

Task Details ? * ☰ ⏏ ⏪ ⏩ ⏹

Name: Scan1 ID: c8745932-1b35-4231-89d7-c014db2b34ff
Comment: Created: Sat May 17 01:00:04 2014
Scan Config: Full and fast ultimate Last Modified: Sat May 24 14:58:36 2014
Alerts:
Schedule: (Next due: over)
Target: net-corporate
Slave:
Status: 2 %
Reports: 1 (Finished: 0)
Observers:
Add to Assets: yes
Notes: 0
Overrides: 0

Scan Intensity
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20

Reports for "Scan1" ? Apply overrides

Report	Threat	Scan Results					Actions
		High	Medium	Low	Log	Info Pos	
Sat May 24 14:58:28 2014 Running	High	22	26	18	109	0	<input type="button" value="⏏"/> <input type="button" value="🔍"/> <input type="button" value="🗑"/>

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

- En el panel inferior podremos observar las vulnerabilidades analizadas por nivel de criticidad (Alto, Medio Bajo), y si pulsamos para visualizar el reporte, los sistemas analizados y la información de cada una de las vulnerabilidades y sus características.
- Una de las opciones más importantes del sistema de reportes es la posibilidad de **exportarlo en formatos altamente compatibles**, como por ejemplo .nbe, que es el fichero nativo de nessus.
- Veremos que **esta capacidad será determinante para su posterior utilización en herramientas de terceros como metasploit.**

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – OpenVAS

Report Summary  Apply overrides 

Result of Task: Scan1 Task

Order of results: by host

Scan started: Sat May 24 14:58:36 2014

Scan ended: Sat May 24 15:31:55 2014

Scan status:

	High	Medium	Low	Log	False Pos	Total	Run Alert	Download
Full report:	22	26	18	110	0	176	 	PDF  
All filtered results:	22	26	0	0	0	48	 	PDF  
Filtered results 1 - 48:	22	26	0	0	0	48	 	PDF  

Análisis de vulnerabilidades

Aplicaciones para el análisis de vulnerabilidades – Nexpose & Retina

- Soluciones que están ganando adeptos, aunque también son de código privado y tienen limitaciones debido a una versión comercial que hay en el mercado, sus desarrolladores son Rapid7 y BeyondTrust respectivamente.
- Aunque son herramientas similares a las vistas, se recomienda al alumno que las instale y las conozca.

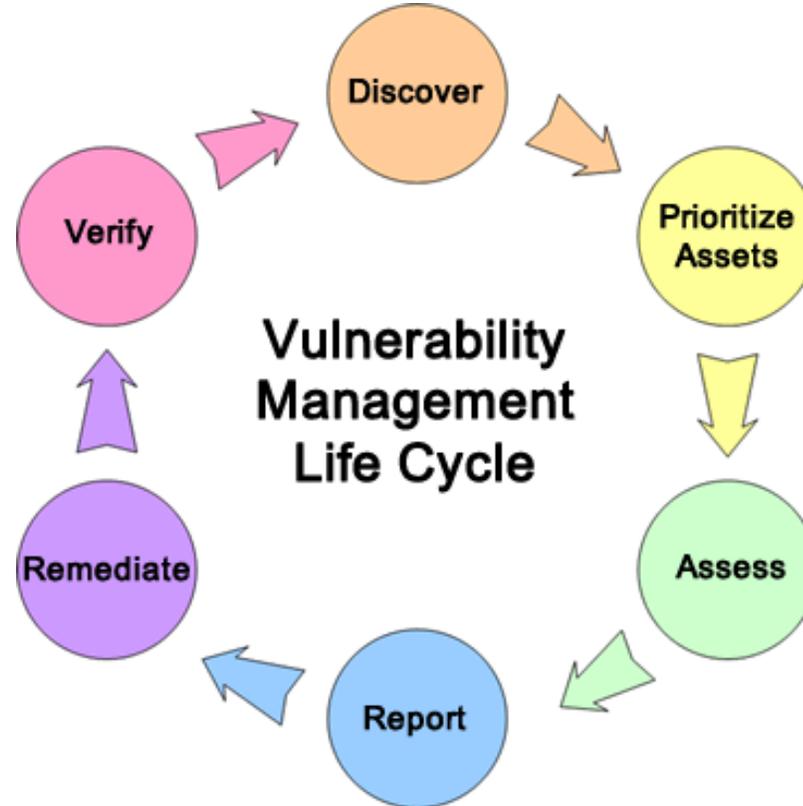
Análisis de vulnerabilidades

Análisis de vulnerabilidades - Conceptos

- Debemos **profundizar más en la catalogación de vulnerabilidades y tipología** de las mismas para poder entender completamente, no sólo las aplicaciones que hemos visto, sino todas aquellas que hay en el mercado.
- **Esto es debido a que cada solución, aunque tiene su propia base de datos de firmas, dispone de unos repositorios que se actualizan con unos servidores internacionales donde se almacenan estas vulnerabilidades.** Ya vimos algunos en el diagrama, pero hay mucho más y con otras funciones, detrás de cada uno de ellos.
- **Cada vulnerabilidad es catalogada y referenciada, y se marca su nivel de criticidad,** para ello hay varios organismos internacionales, la mayoría americanos, encargados de este cometido .

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – Ciclo de vida



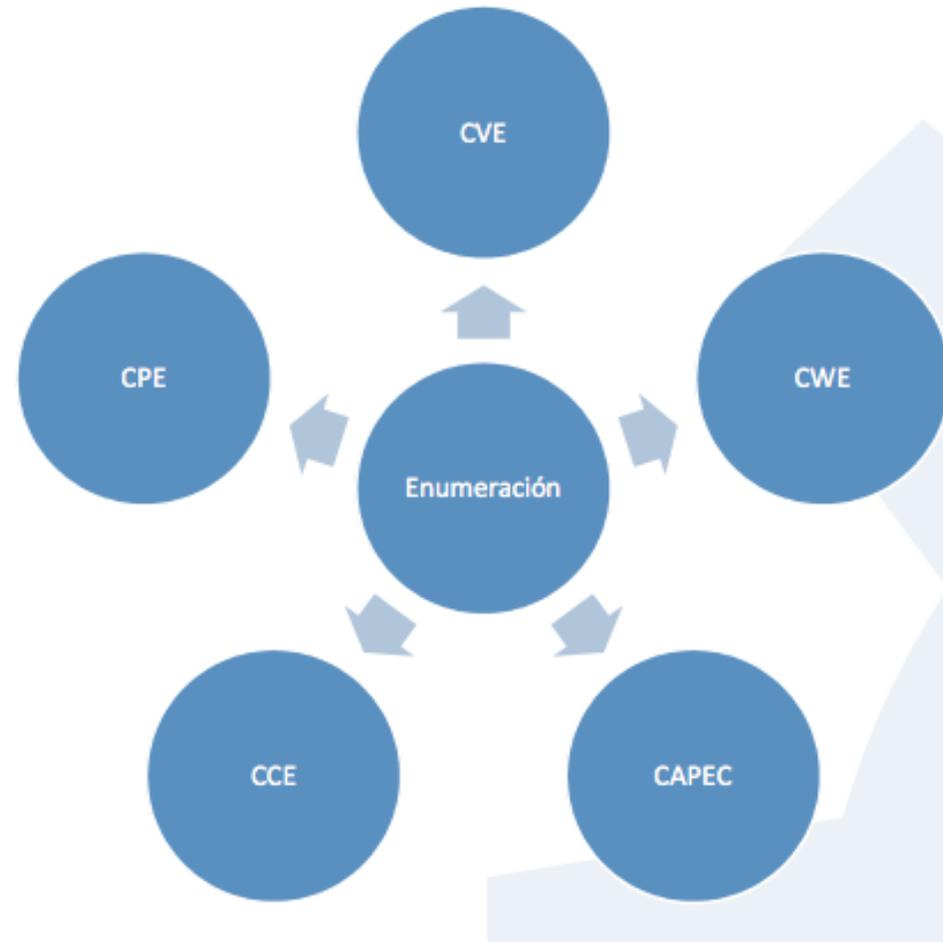
Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – Ciclo de vida

- **Enumeración de la vulnerabilidad:** una vez que la vulnerabilidad esta publicada y es conocida, independientemente que este solucionada o no, **existe una organización que se encarga de catalogarlas de manera estandarizada**, por lo que cada vulnerabilidad estará referida de manera única. **Este organismo es el Mitre.**

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – Ciclo de vida



Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVE

- **Common Vulnerability Exposure**
- El Mitre es un organismo compuesto por profesionales de las principales corporaciones, por ejemplo NSA, IBM, Cisco, SANS Institute, que se encarga de catalogar las vulnerabilidades y dotarlas de una nomenclatura que las referencie de forma coherente independientemente del sistema operativo y características internas de la misma y del objetivo que afecte.
- El organismo se puede consultar desde la web <http://cve.mitre.org/>, donde está la base de datos completa de todas las vulnerabilidades y su código.

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVE

■ Estructura del código:

- Si la vulnerabilidad **ha sido revisada y aceptada**, estará englobada dentro de la **categoría CVE**, si aún no está aceptada ni revisada, pero ya se ha dado de alta como tal, estará en la **categoría CAN** (Candidate).
- La categoría **Candidate** ya está en desuso, y no es utilizada en la actualidad, pero es muy probable que aún nos encontremos vulnerabilidades referenciadas mediante esta nomenclatura.
- La numeración es el año, un guion y un número consecutivo que asigna el organismo, por ejemplo **CVE 2010-0345**, o **CAN 2010-3678** (que una vez aceptada pasar a ser **CVE 2010-3678**)

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVE

- **NVD (NIST) <http://nvd.nis.gob> enlaza la base de datos CVE a otras iniciativas que veremos a continuación, por lo que nos ofrece mucha más información que la simple lista CVE.**
- **INCIBE ha desarrollado una ardua labor traduciendo las vulnerabilidades al español, bajo un acuerdo realizado con el NIST, organización que mantiene la NVD.**

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CWE

- **Common Weakness Enumeration** es otro estándar desarrollado por los **mismos responsables que el CVE, Mitre**. Este estándar relativo, decimos relativo, porque no está tan implementado como su hermano CVE, y a su amparo han surgido otras propuestas que también se están utilizando.
- **CWE se encarga de categorizar las vulnerabilidades en grupos de características comunes entre las vulnerabilidades.**
- **CWE es quizás el sistema de agrupación de vulnerabilidades más extenso del mercado, tiene más de 680 categorías para clasificar las debilidades en el software**

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CAPEC

- **Common Attack Pattern Enumeration and Classification:** se encarga de **clasificar los vectores de ataque**. Un vector de ataque es todo aquel frente tecnológico, tras el cual se ha descubierto una vulnerabilidad y mediante el cual se puede explotar, un claro ejemplo sería el spoofing, tenemos una vulnerabilidad, por ejemplo sidehijacking, que afecta a las cookies y los navegadores y que en una red local puede ser explotada mediante spoofing, el spoofing sería pues el vector de ataque.
- **CAPEC está desarrollado por los mismos reponsables que las dos anteriores iniciativas, Mitre, y está compuesto de 460 elementos** divididos según la siguiente estructura, 6 vistas, 68 categorías y 386 vectores de ataque

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CCE

- **Common Configuration Enumeration:** también forma parte de los **proyectos administrados por Mitre**, como veis es un organismo volcado en el diseño de una estructura única para el manejo de vulnerabilidades, y todo lo que gira alrededor de las mismas.
- **CCE se encarga de identificar de manera inequívoca los diferentes aspectos de configuración de los sistemas operativos y aplicaciones**, que tienen relación con la seguridad o con vulnerabilidades

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CPE

- **Common Platform Enumeration:** también promocionado por el Mitre, CPE se encarga de representar a los sistemas operativos y aplicaciones mediante un identificador.
- En realidad CPE es un “lenguaje” (a través de URI) que quiere unificar varios factores en una misma declaración, y poder representar productos de software, sistemas operativos, y cualquier objeto de software mediante una única instrucción:
 - `<cpe-item name="cpe:/a:mcafee:e-business_server:3.5">`

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVSS

- **Common Vulnerability Scoring System: una de las iniciativas más seguidas y aclamadas, después de la catalogación a través de ID CVE. CVSS, dirigida por el FIRST. Es un "Sistema de puntuación de vulnerabilidades", esto quiere decir que se dedica a asignar un valor a cada una de ellas, y este valor representará la criticidad de la misma y por lo tanto el nivel de riesgo.**
- **Dispone de una serie de métricas que veremos a continuación y que son: Métricas base, temporales y de entorno.**

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVSS – M Base

- **AV (Acces Vector):** Local (L), adyacente (A), remoto (N)
- **AC (Access Complexity) -> Complejidad de Acceso:** L, M y H
- **AU (Authentication) -> Autenticación:** None (N), Simple (S), Múltiple (M)
- **Tiene otros tres que afectan al CIA y que pueden tener el valor:** N (ninguno) P (parcial) o C (Completo)
- **Un ejemplo del dato completo:**
 - AV:(L,A,N)/AC:(H,M,L)/AU:(M,S,N)/C:(N,P,C)/I:(N,P,C)/A:(N,P,C)

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVSS – M Temporales

- En este caso miden la probabilidad de que la vulnerabilidad mute a través del tiempo, según la aparición de herramientas o métodos para su explotación.
- **Explotabilidad (E):** ND = Valor no definido, U = No probado, POC = Prueba de Concepto, F = Funcional y H = Alto
- **Nivel de Solucion (RL):** ND = Valor no definido, U = No Hay, W = WorkAround, TF = Solución temporal y OF = Parche Oficial
- **Confiabilidad de la fuente (RC):** ND = Valor no definido, C = Fuente Confirmada, UR = Fuente de credibilidad no investigada y UC = No confirmada
- **Un ejemplo de su representación:**
 - E:(U,POC,F,H,ND)/RL:(OF,TF,W,U,ND)/RC:(UC,UR,C,ND)

Análisis de vulnerabilidades

Análisis de vulnerabilidades – Conceptos – CVSS – M Entorno

- Estos valores determinan la influencia del entorno tecnológico en la vulnerabilidad que se está tratando.
- **Daño potencial colateral (CPD):** Daño causado en los dispositivos que puede provocar su malfuncionamiento o pérdida total: ND = Valor no definido, L = Bajo, LM = Bajo / Medio, MH = Medio / Alto y H = Alto
- **Distribución de objetivos (TD):** Nos ofrece un dato referente al total de sistemas existentes en un entorno y el nivel, entre todos ellos, de afectados por la vulnerabilidad: ND = Valor no definido, L = Bajo, M = Medio y H = Alto.
- **Requisitos de Seguridad (CR):** Se establece un dato sobre la importancia de la Integridad, Confiabilidad y Disponibilidad de un sistema afectado: ND = Valor no definido, L = Bajo, M = Medio y H = Alto.
- Representación:
 - CDP:(N,L,LM,MH,H,ND)/TD:(N,L,M,H,ND)/CR:(L,M,H,ND)

Análisis de vulnerabilidades

Bases de datos de vulnerabilidades – NIST

- Sin duda la base de datos de vulnerabilidades “por excelencia”. Contiene toda la información necesaria para conocer todos los detalles de una vulnerabilidad salvo la información para explotarla.
- De obligada consulta cuando se descubre un CVE vulnerable en una aplicación de análisis.

Análisis de vulnerabilidades

Bases de datos de vulnerabilidades – Secunia

- **Una de las exponentes y referencia a la hora de identificar vulnerabilidades.** La base de datos de Secunia se ha hecho su "hueco" en este mundo escalando posiciones hasta llegar a lo más alto, pero todo tiene su contra, **aunque la información es gratuita, no podemos descargarnos la base de datos, para eso tienen su propio producto.**

<http://secunia.com>

Análisis de vulnerabilidades

Bases de datos de vulnerabilidades – SecurityFocus

- **Una de las más antiguas y con más prestigio. Lo mejor de esta base de datos es toda la información que ofrece, entre ella:**
 - Apartado de discusión
 - Exploit relacionado con la vulnerabilidad (si existiese)
 - Solución a la vulnerabilidad
 - Referencias
- **Es de visita obligatoria para estar al día de las vulnerabilidades actuales**

<http://www.securityfocus.com/>

Análisis de vulnerabilidades

¿PREGUNTAS?

