Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Nessus: Un pontente escáner de redes. How-To Install and Configuring

Per **LauraCeldranS**, ***LauraCS*** (http://laura.celdran.name)

Creado el 26/05/2005 09:08 modificado el 26/05/2005 09:26

> ***Nessus*** es un potente **escáner de redes** de Software Libre que consta de dos partes: cliente y servidor; éstas pueden estar instaladas en las misma máquina por simplicidad (en este post así se expone).
>
> Es interesante decir que con nessus se pueden grabar informes donde hay enlaces que explican que tipo de vulnerabilidad encontrada, cómo "explotarla" y cómo "evitarla"
>
> En este artículo se describe brevemente su **puesta en marcha** y **configuración** de forma muy sencilla en cinco pasos.

Nessus es un potente escáner de redes de Software Libre. Consta de dos partes (cliente/servidor) que pueden estar instaladas en las misma máquina por simplicidad (en este post así se expone).

Se debe comentar que si el ataque se hace hacia localhost lo que se consigue es auditar nuestra propia máquina.

Cuando Nesuss finaliza el escaneo genera unos informes muy útiles si se sabe aprovechar e interpretar la información obtenida.

La distribución de Nessus consta de cuatro ficheros básicos: las *librerías del programa*, las librerías *NASL* (Nessus Attack Scripting Language), el *núcleo* de la aplicación y sus *plugins*; es necesario compilar en este orden cada una de esas partes. Puede que tenga alguna dependencia, así que ojillo.
Pasos

1. Para los que usáis apt. Ya sabéis *apt-get install nessus*, *apt-get install nessusd* (y se instalan solas todas las dependencias) y luego os descargáis de la página de Nessus (http://www.nessus.org/[1]) los plugins y los instaláis en la carpeta de plugins (dentro de la carpeta nessus: */nessus/plugins*).

   Para los que no, instalar en el orden indicado arriba los fuentes necesarios (http://www.nessus.org[2])

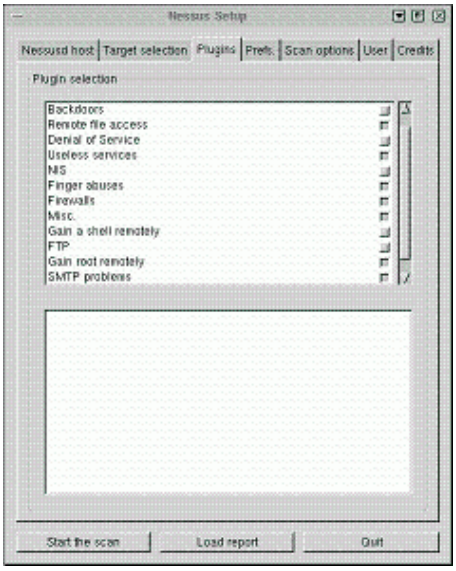
2. Configurar el programa: Archivo de configuración del servidor (la configuración por defecto es completa y válida, entre otras cosas escanea desde el puerto 0 al 15000): *cd /etc/nessus/nessusd.conf*

3. Crear un usuario que sea el que pueda lanzar el programa, para ello siga las instrucciones tras poner el comando: *nessus-adduser*.

   Entre más opciones, elegir que el sistema sea de login/password, porque simplifica el escenario; además elegir que pueda accederse al servidor desde cualquier red (por simplificar): *default accept*.

4. Arrancar en background el servidor: *nessusd -D* o *nessusd --background*

5. Iniciar el cliente en modo gráfico (también se puede iniciar en modo comando, para esto consultar ayuda: nessus man): *nessus*



p

En la pestaña de Plugins (son los ataques) seleccionar todos si es que se desea probar con todos.

En Target Selection indicar la dirección IP de la máquina a escanear.En Nessusd Host, se indican los datos que se han añadido en la creacción del usuario (login/password, etc)

Nota: La configuración expuesta es muy sencilla pero se insta a los que provéis este programa a consultar los manuales para depurar mejor la herramienta y así obtener mejores resultados.

Espero que os sea útil. Para más información ...http://laura.celdran.name[3]

Lista de enlaces de este artículo:

1. http://www.nessus.org/
2. http://www.nessus.org
3. http://laura.celdran.name

E-mail del autor: laura _ARROBA_ laura.celdran.name
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=2193