INSTALACION DE NESSUS

Pero que es Nessus
Fuente Wikipedia

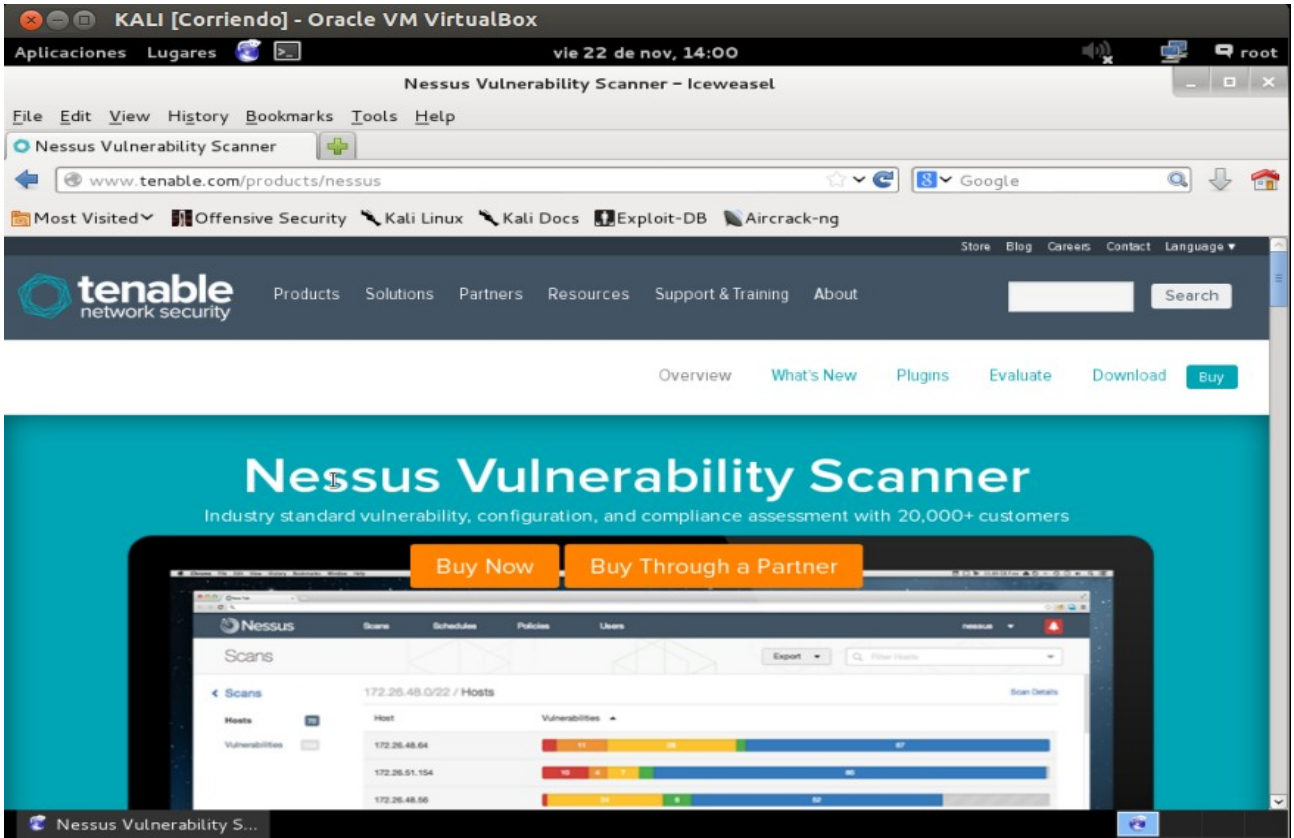
Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus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

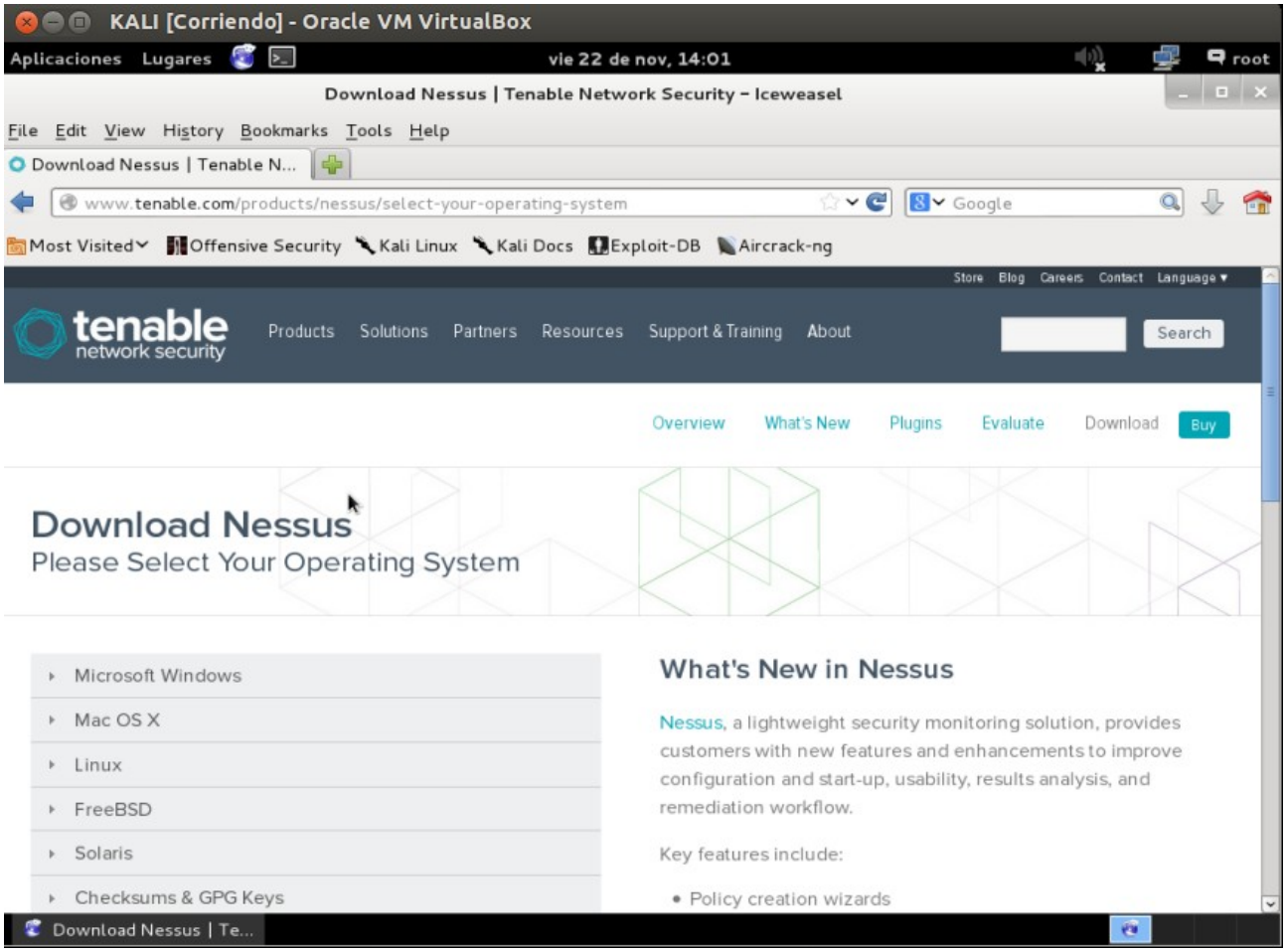
Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

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



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.

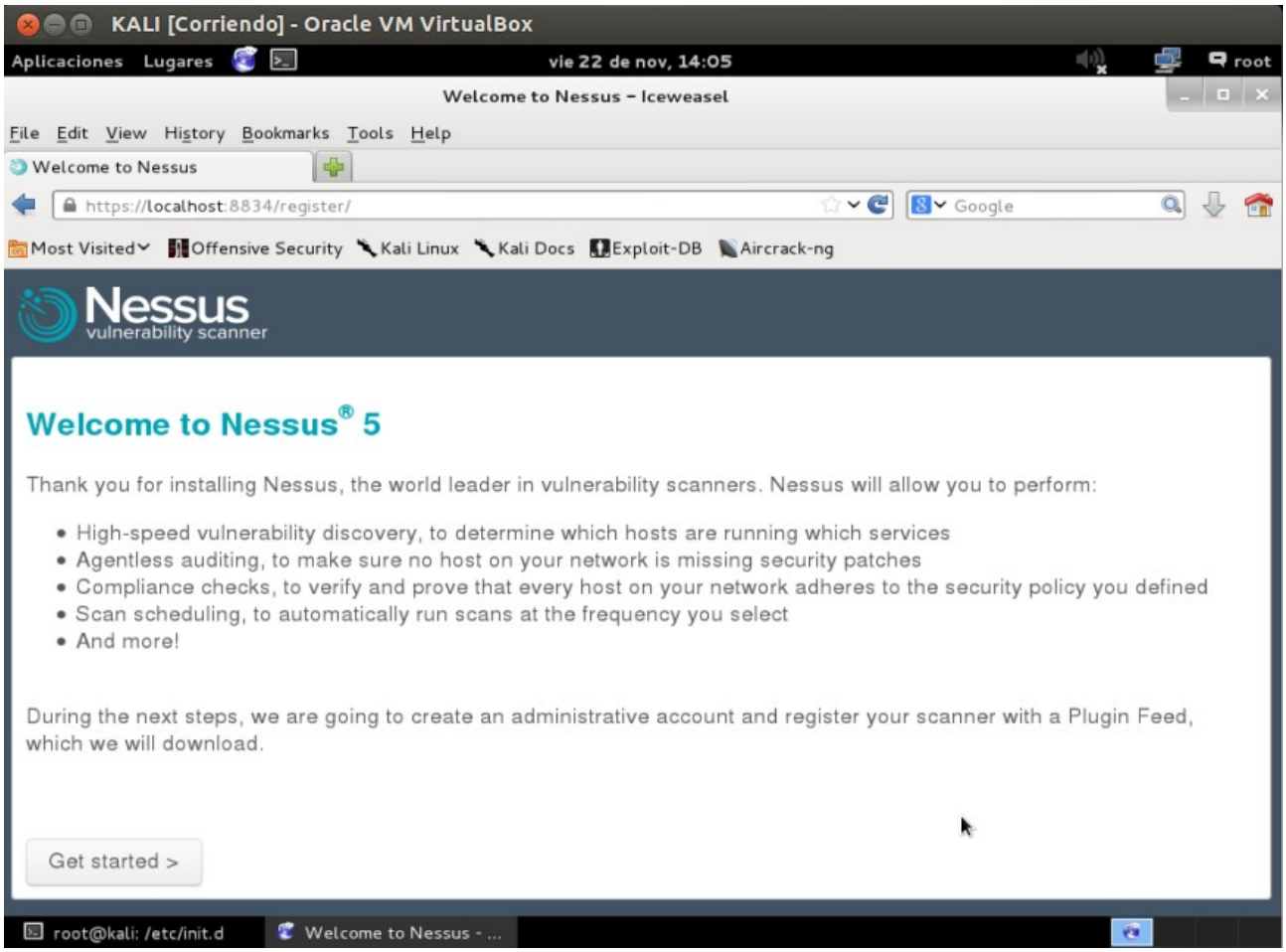
Ahora hay que iniciar Nessus
Para eso nos diridimos a /etc/init.d ./nessusd start

```
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                  rcS               sslh
bluetooth                hdparm                        mysql                    README            stunnel4
bootlogs                 hostname.sh                   nessusd                  reboot            sudo
bootmisc.sh              hwclock.sh                    networking               rlinetd           thin
checkfs.sh               iodined                       network-manager          rmnologin         truecrypt
checkroot-bootclean.sh   kbd                           nfs-common               rpcbind           udev
checkroot.sh             keyboard-setup                nginx                    rsync             udev-mtab
console-screen.sh        killprocs                     ntp                      rsyslog           umountfs
console-setup            kmod                          openvas-administrator    samba             umountnfs.sh
cron                     lvm2                          openvas-manager          saned             umountroot
cryptdisks               metasploit                    openvas-scanner          screen-cleanup    urandom
cryptdisks-early         miredo                        openvpn                  sendsigs          x11-common
darkstat                 motd                          pcscd                    single
dbus                     mountall-bootclean.sh         postgresql               skeleton
root@kali:/etc/init.d# ./nessusd start
```

Y ya esta iniciado
Nos dirigimos al navegador y colocar

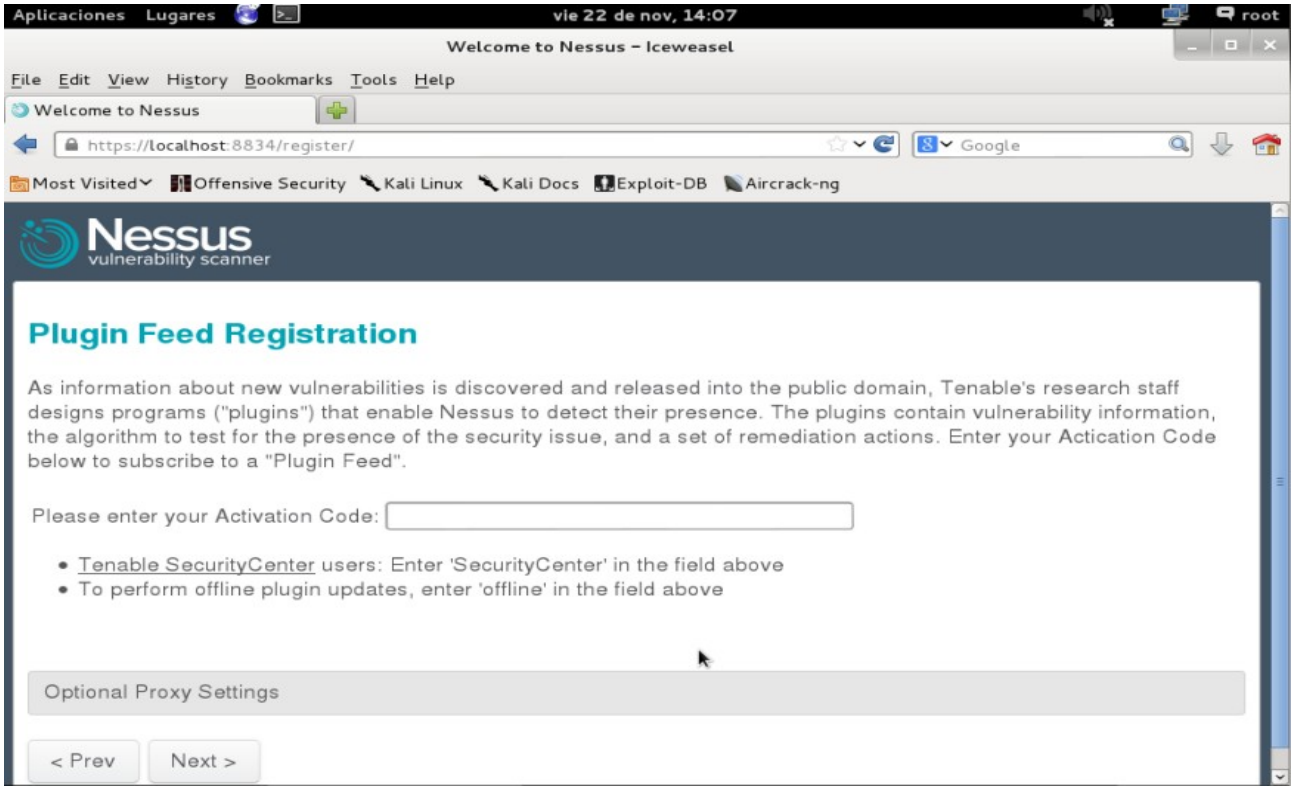
https://localhost:8834

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

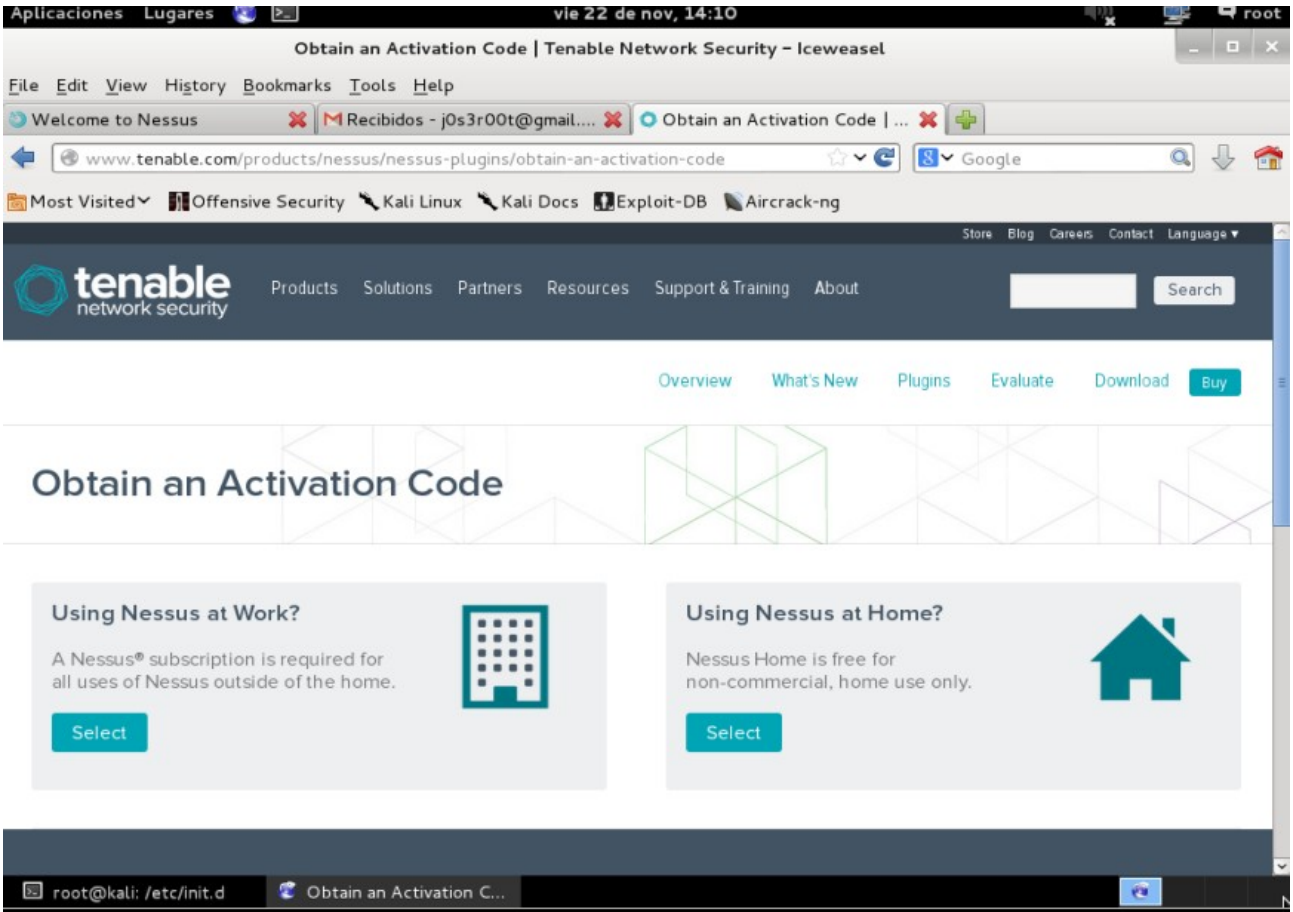


Clikamos Get started

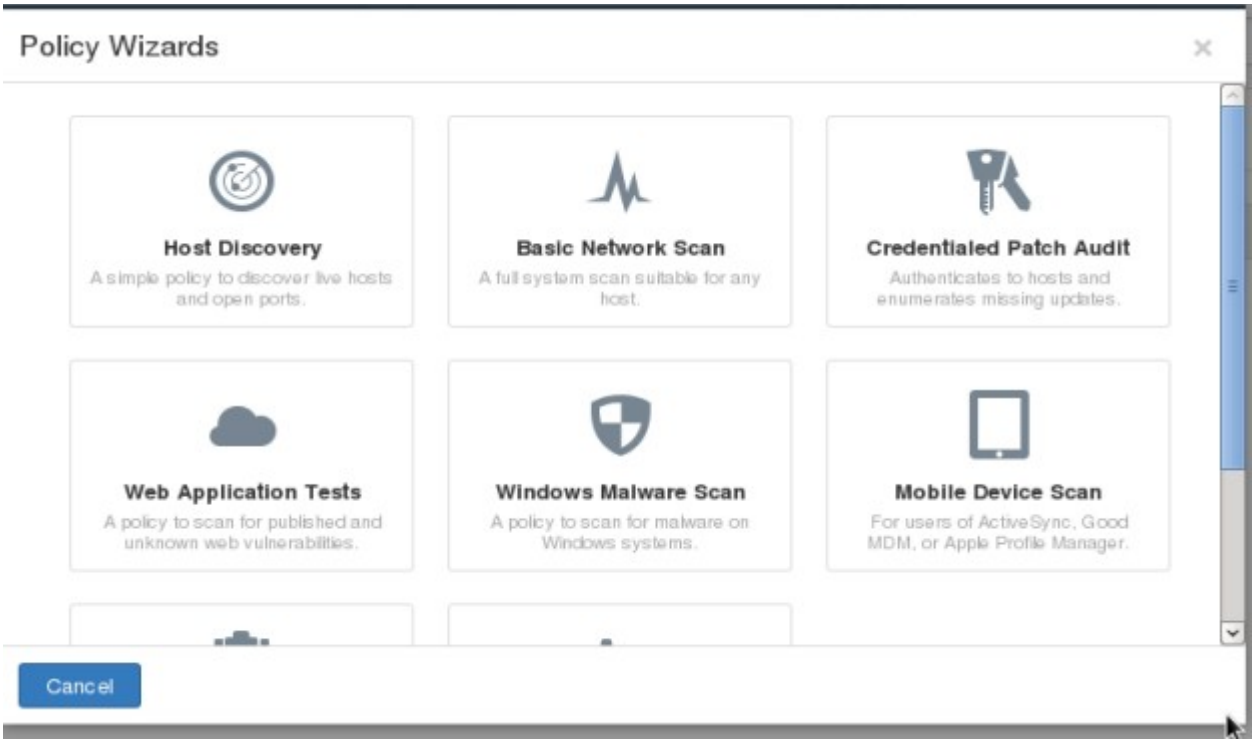
Y a continuacion nos pide
Login & Password
Los rellenamos y Next
En el paso siguiente nos pide el codigo de activacion.



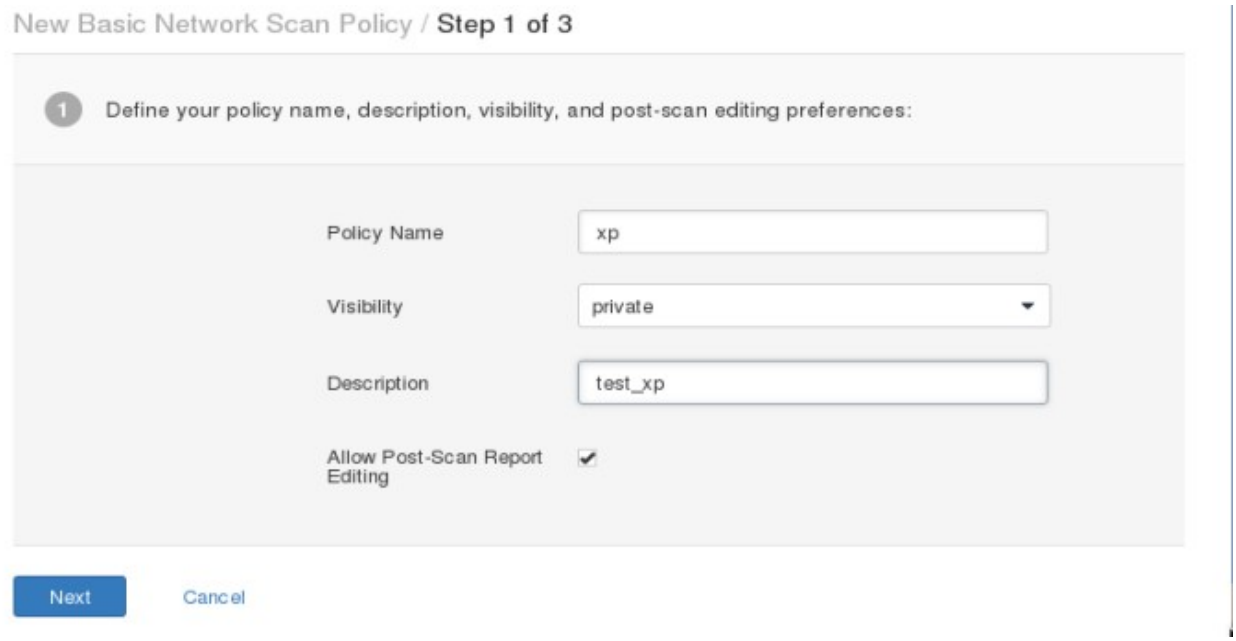
El link para obtener el codigo:
http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code
Y seleccionamos: Using Nessus at Home?



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

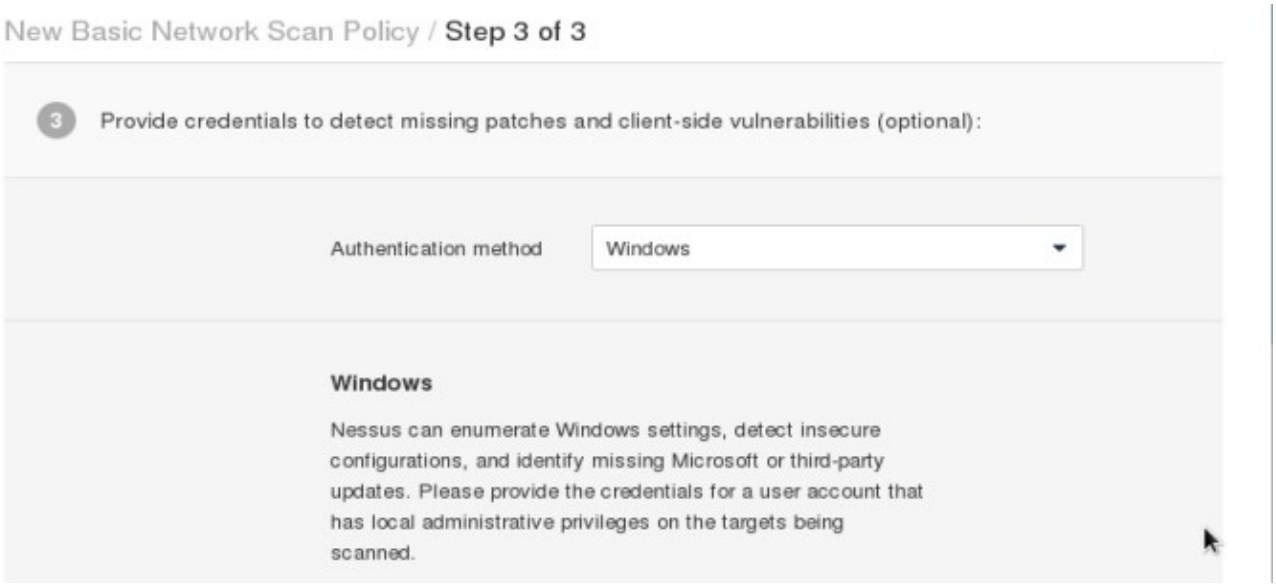


En este caso Basic Network Scan



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

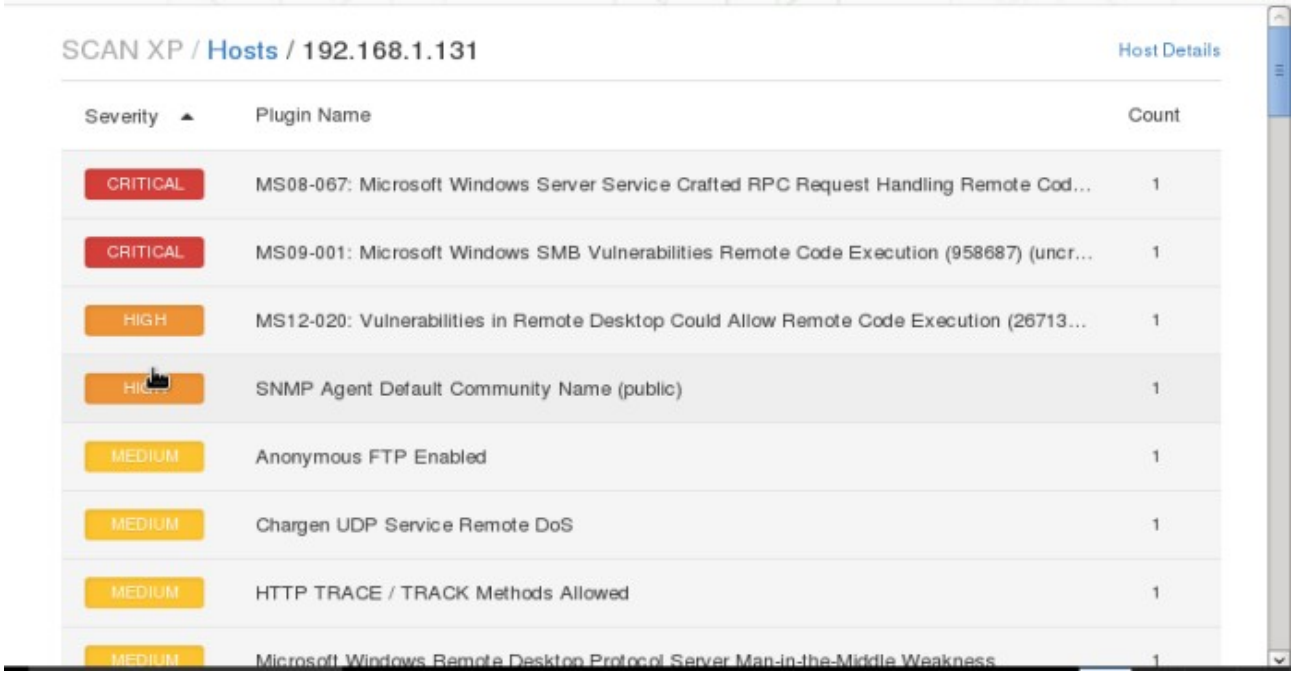


En method windows, ya que la maquina es un Windows

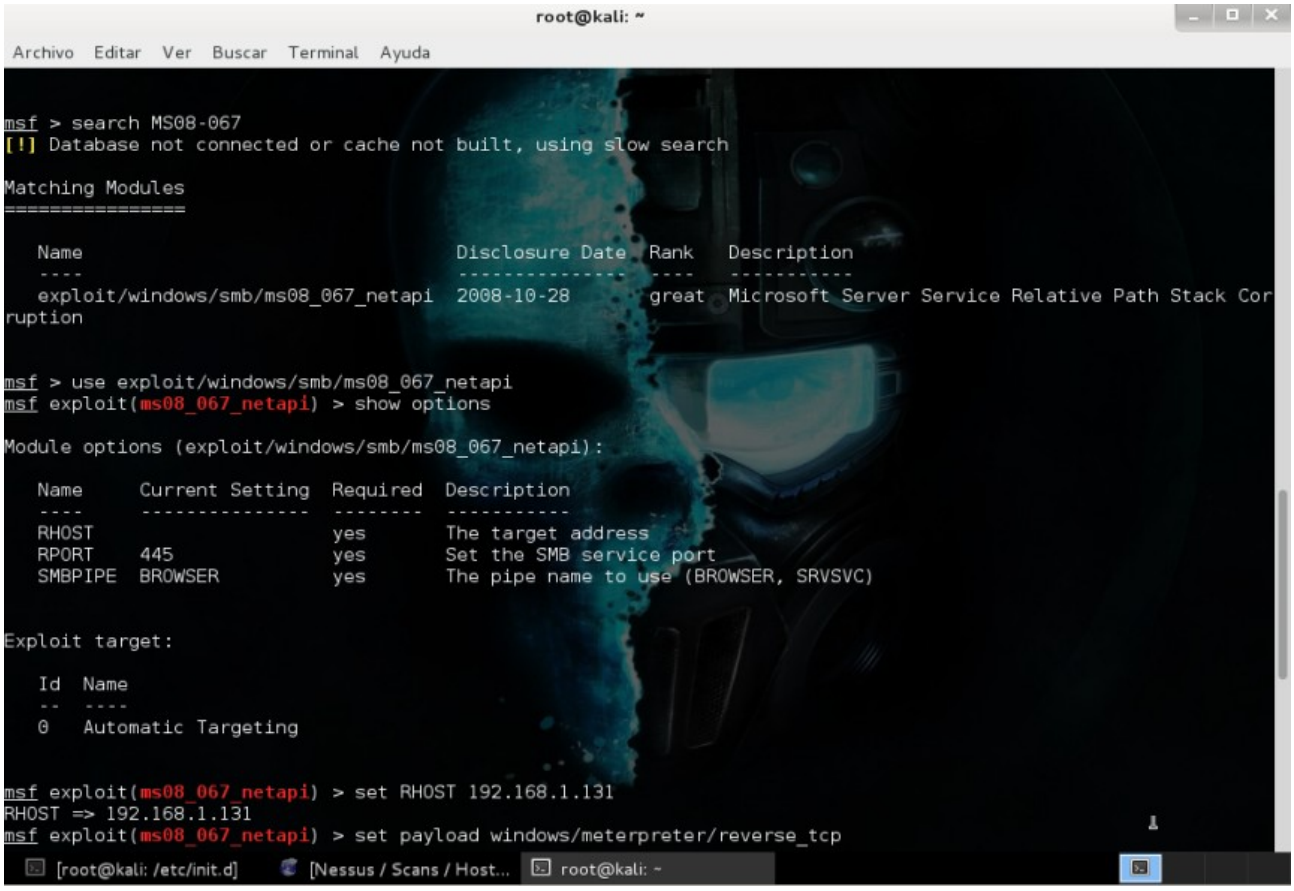
Siguiendo inportante en Targets el host a escanear ejemplo: 192.168.1.120

Clikamos Launch y se pondra a escanear.

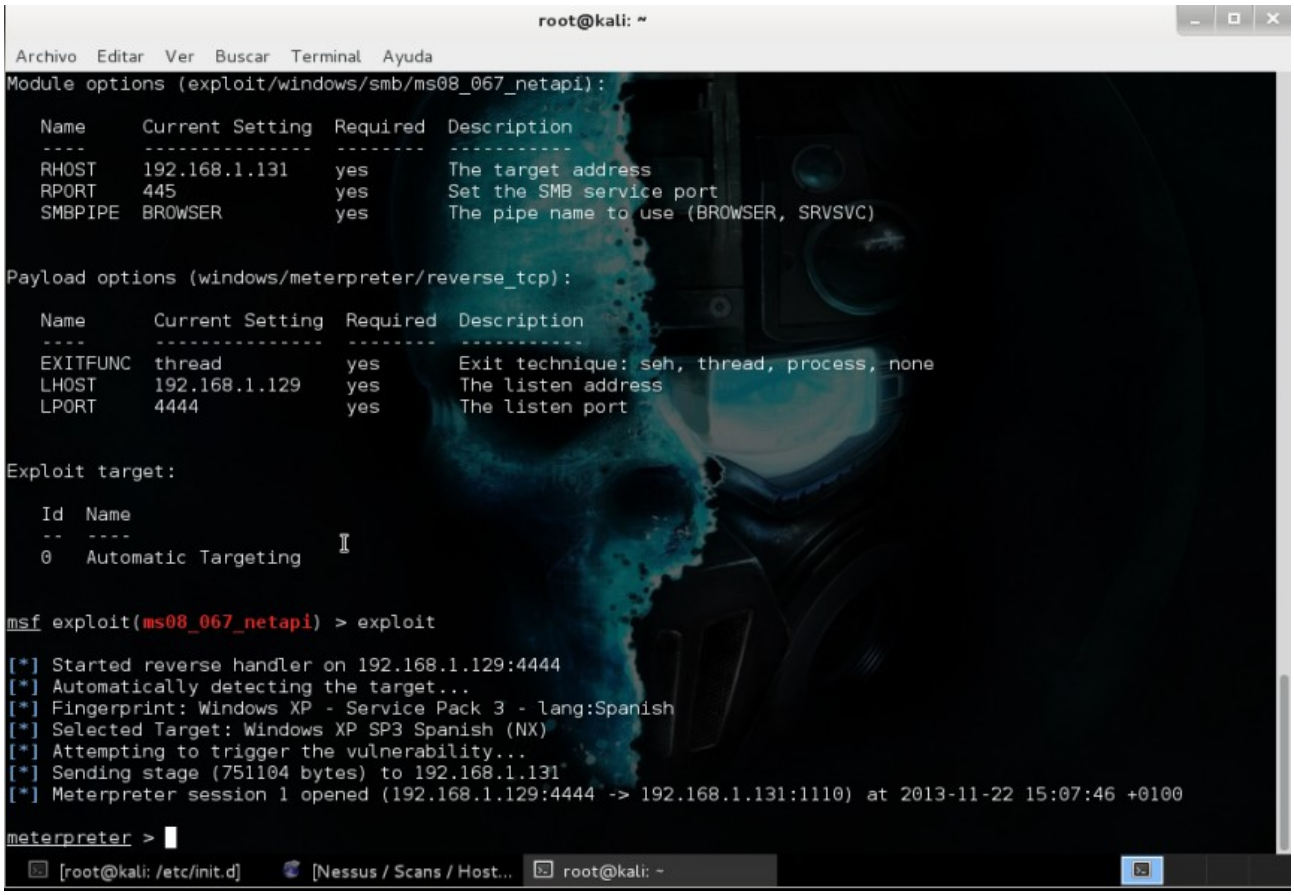
Muestro un escaneo ya finalizado



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



Una vez que e configurado las variables
Lanzo exploit



Y ya tengo mi sesion de metrepreter.

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

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