

## Análisis de vulnerabilidades con Nexpose en Backtrack

En el laboratorio actual usted instalará la herramienta Nexpose en Linux para realizar un escaneo de puertos y analizar las vulnerabilidades presentes..

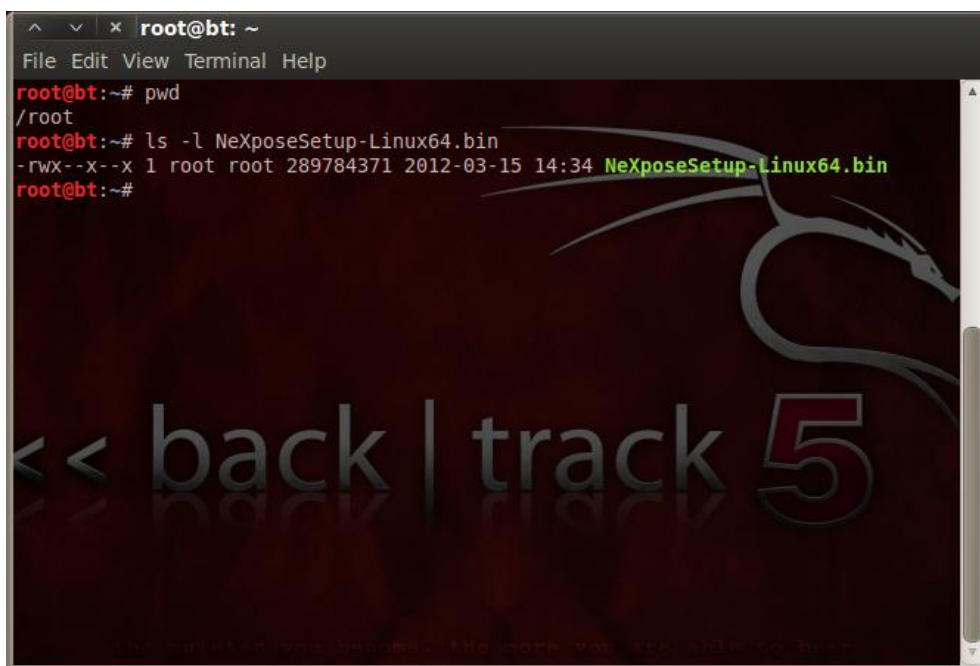
**Nota:** Para la ejecución de los laboratorios se requiere un PC con sistema operativo Backtrack 5 y conexión directa a Internet, por favor verifique con su instructor si es necesario que cuenta con los permisos de acceso pertinentes.

### Ejecución paso a paso

En este laboratorio usaremos la herramienta Nexpose de la empresa Rapid 7, la cual no viene incluida por defecto con Backtrack Linux, para realizar un análisis de vulnerabilidades de un equipo indicado por su instructor.

El primer paso es instalar Nexpose desde el instalador provisto a usted por su instructor (o si su conexión lo permite descárguelo desde el sitio web de Rapid 7 <http://www.rapid7.com/products/nexpose-community-edition.jsp> , tome en cuenta que es un archivo grande, más de 200MB).

Transfiera el archivo de Nexpose a su sistema Backtrack y ejecute el programa de instalación como el usuario root, para este laboratorio asumiremos que el instalador es para una plataforma de 64 bits y se encuentra en la ubicación /root:



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# pwd
/root
root@bt:~# ls -l NeXposeSetup-Linux64.bin
-rwx--x--x 1 root root 289784371 2012-03-15 14:34 NeXposeSetup-Linux64.bin
root@bt:~#
```

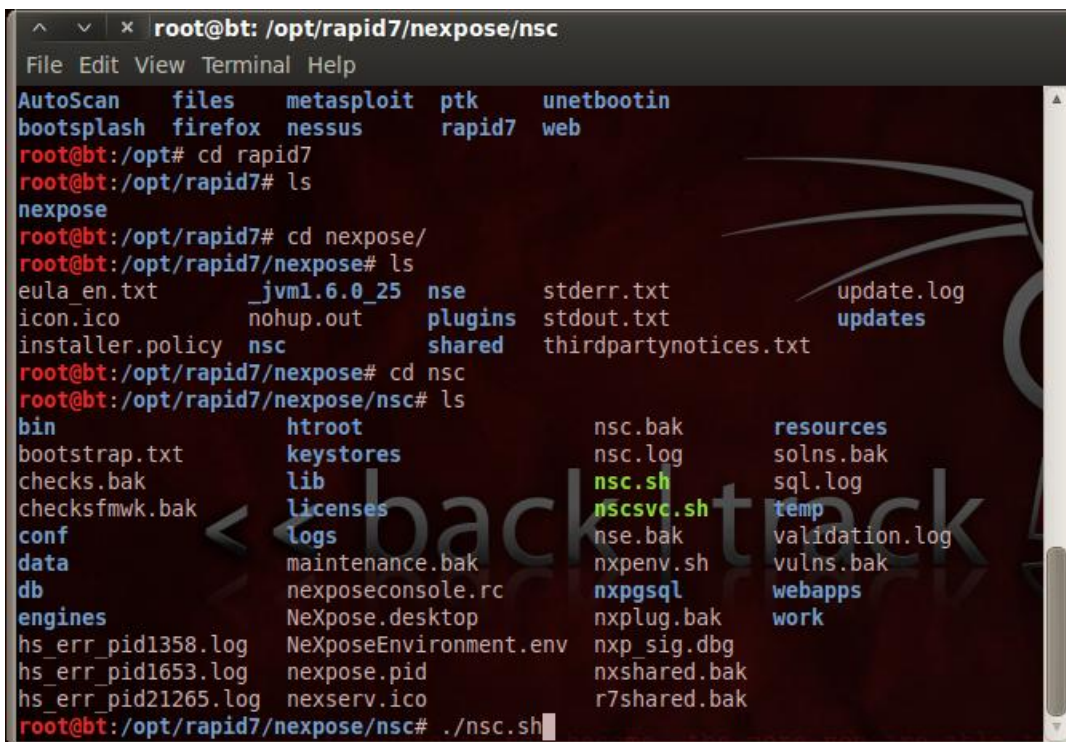
Para poder ejecutar el instalador cerciórese de contar con el permiso respectivo, sino agréguelo con el comando `chmod`.

```
chmod u+x NeXposeSetup-Linux64.bin
```

Y ejecute el archivo de instalación:

```
./NeXposeSetup-Linux64.bin
```

El instalador es gráfico y sencillo de usar, siga las instrucciones en pantalla para instalar Nexpose.



```

root@bt: /opt/rapid7/nexpose/nsc
File Edit View Terminal Help
AutoScan files metasploit ptk unetbootin
bootsplash firefox nessus rapid7 web
root@bt:/opt# cd rapid7
root@bt:/opt/rapid7# ls
nexpose
root@bt:/opt/rapid7# cd nexpose/
root@bt:/opt/rapid7/nexpose# ls
eula_en.txt _jvm1.6.0_25 nse stderr.txt update.log
icon.ico nohup.out plugins stdout.txt updates
installer.policy nsc shared thirdpartyntices.txt
root@bt:/opt/rapid7/nexpose# cd nsc
root@bt:/opt/rapid7/nexpose/nsc# ls
bin htroot nsc.bak resources
bootstrap.txt keystores nsc.log solns.bak
checks.bak lib nsc.sh sql.log
checksfmwk.bak licenses nscsvc.sh temp
conf logs nse.bak validation.log
data maintenance.bak nxpenv.sh vulns.bak
db nexposeconsole.rc nxpgsql webapps
engines NeXpose.desktop nxplug.bak work
hs_err_pid1358.log NeXposeEnvironment.env nxp_sig.dbg
hs_err_pid1653.log nexpose.pid nxshared.bak
hs_err_pid21265.log nexserv.ico r7shared.bak
root@bt:/opt/rapid7/nexpose/nsc# ./nsc.sh

```

Una vez instalado, cámbiese al directorio de instalación (usualmente `/opt/rapid7/nexpose`). Para iniciar la consola deberá arrancar el daemon `nsc`, ubicado en la subcarpeta del mismo nombre:

Cuando el daemon termine de inicializarse deberá observar algo como esto en la línea de comandos (la primera vez puede tomar varios minutos debido a que se compila la base de vulnerabilidades):

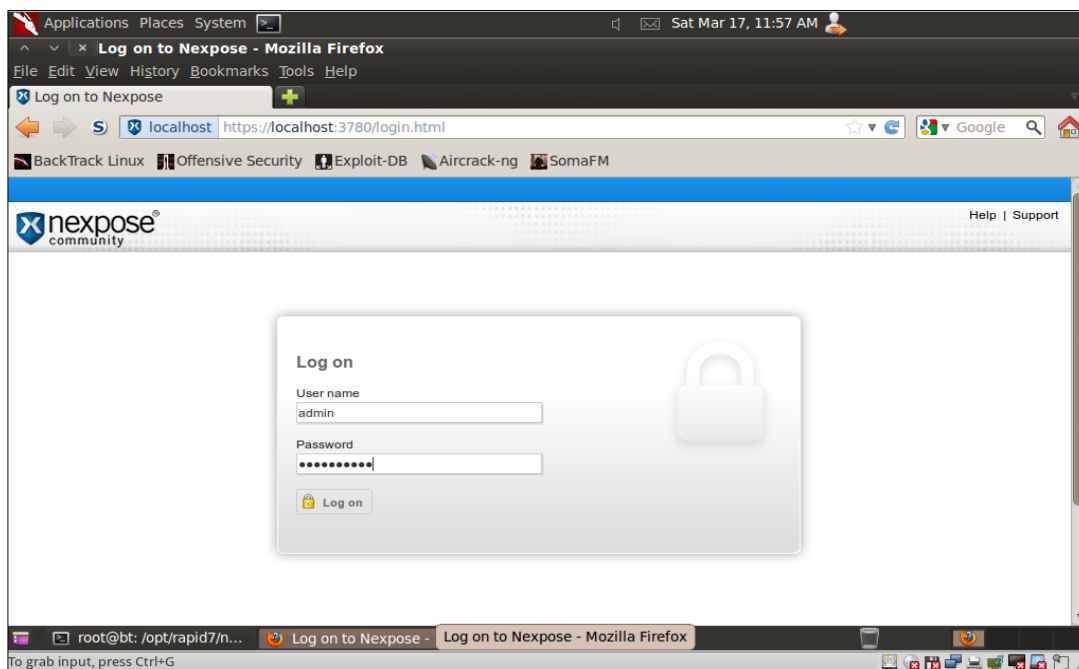
```

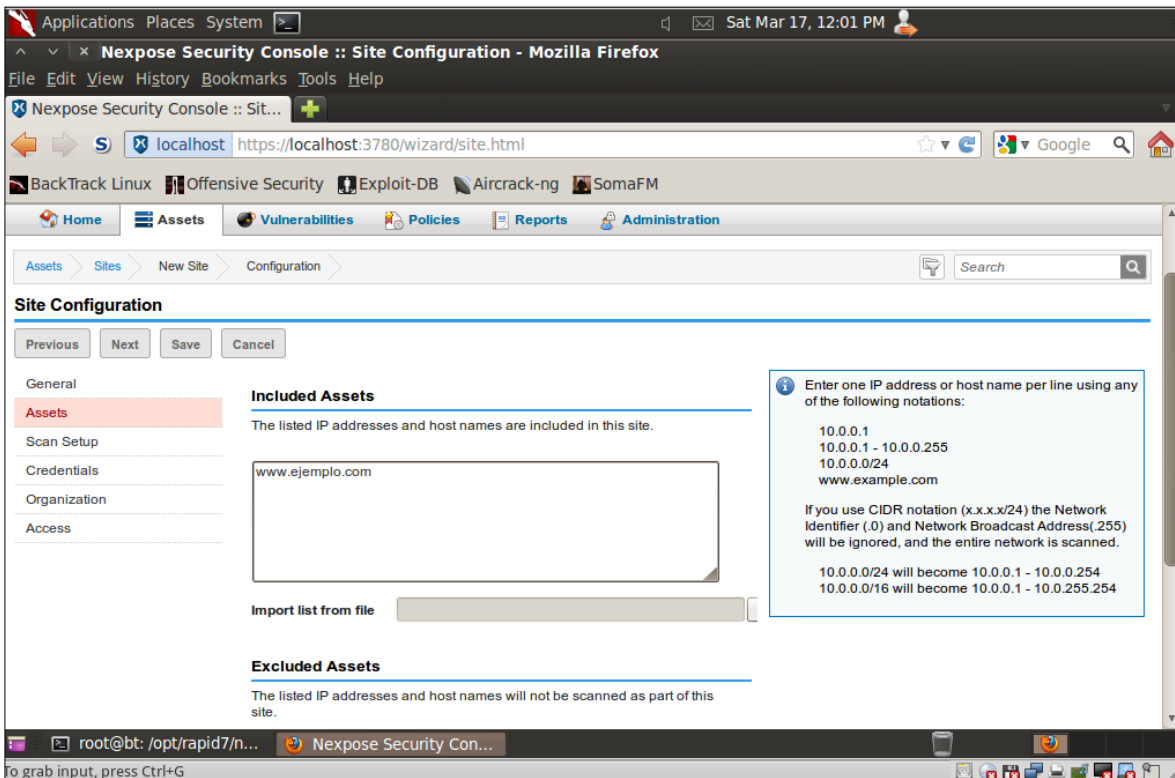
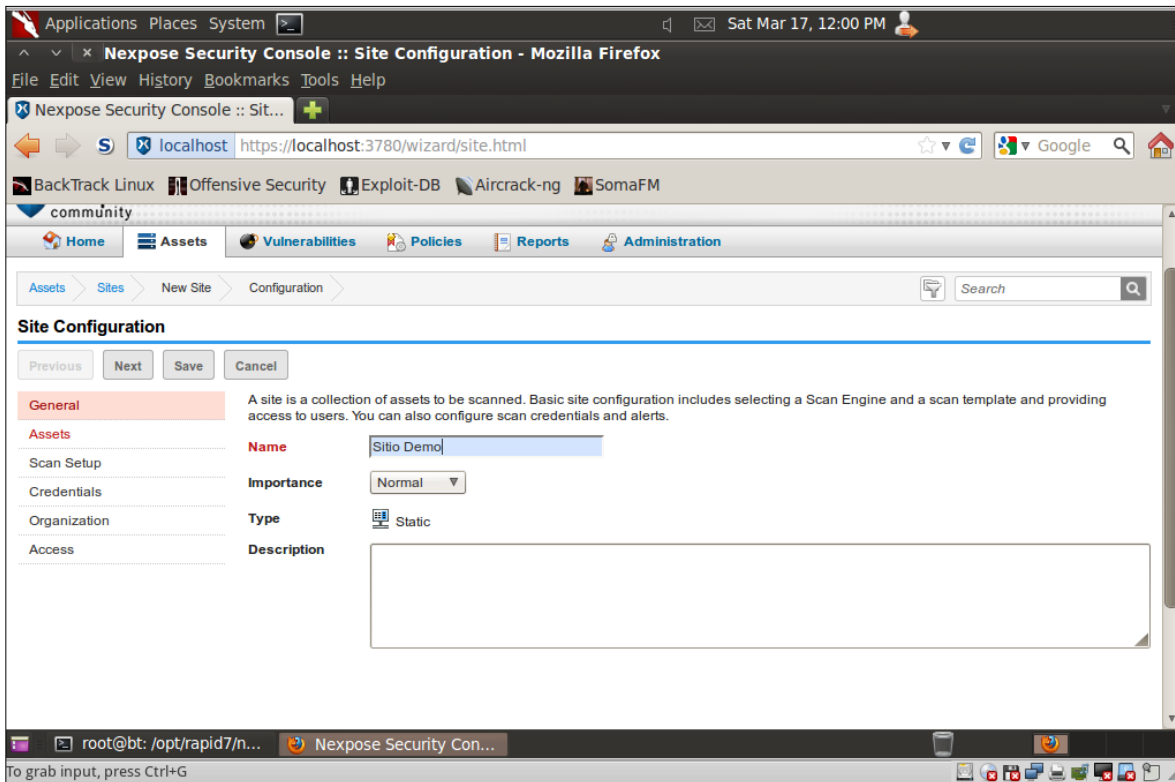
root@bt: /opt/rapid7/nexpose/nsc
File Edit View Terminal Help
Nexpose 2012-03-17T16:54:06 Loading scheduled data warehouse export jobs...
Nexpose 2012-03-17T16:54:06
> JVM memory pool Code Cache (init = 2555904(2496K) used = 4573248(4466K) committed = 5111808(4992K) max = 50331648(49152K))
Nexpose 2012-03-17T16:54:06 JVM memory pool Par Eden Space (init = 6815744(6656K) used = 16625384(16235K) committed = 17432576(17024K) max = 17432576(17024K))
Nexpose 2012-03-17T16:54:06 JVM memory pool Par Survivor Space (init = 786432(768K) used = 265952(259K) committed = 2162688(2112K) max = 2162688(2112K))
Nexpose 2012-03-17T16:54:06 JVM memory pool CMS Old Gen (init = 260046848(253952K) used = 707899136(691307K) committed = 1774329856(1732744K) max = 1947467776(1901824K))
Nexpose 2012-03-17T16:54:06 JVM memory pool CMS Perm Gen (init = 21757952(21248K) used = 45838480(44764K) committed = 74129408(72392K) max = 167772160(163840K))
Nexpose 2012-03-17T16:54:06 Enabling resource self protection
Nexpose 2012-03-17T16:54:06 JVM Warning Threshold set at 1.7 GB out of 1.8 GB from Tenured Generation
Nexpose 2012-03-17T16:54:06 JVM Reaction Threshold set at 1.8 GB out of 1.8 GB from Tenured Generation
NSC 2012-03-17T16:54:10 Secure web interface ready.
NSC 2012-03-17T16:54:10 Browse to https://localhost:3780/
NSC 2012-03-17T16:54:10 Server started in 5 minutes 47 seconds

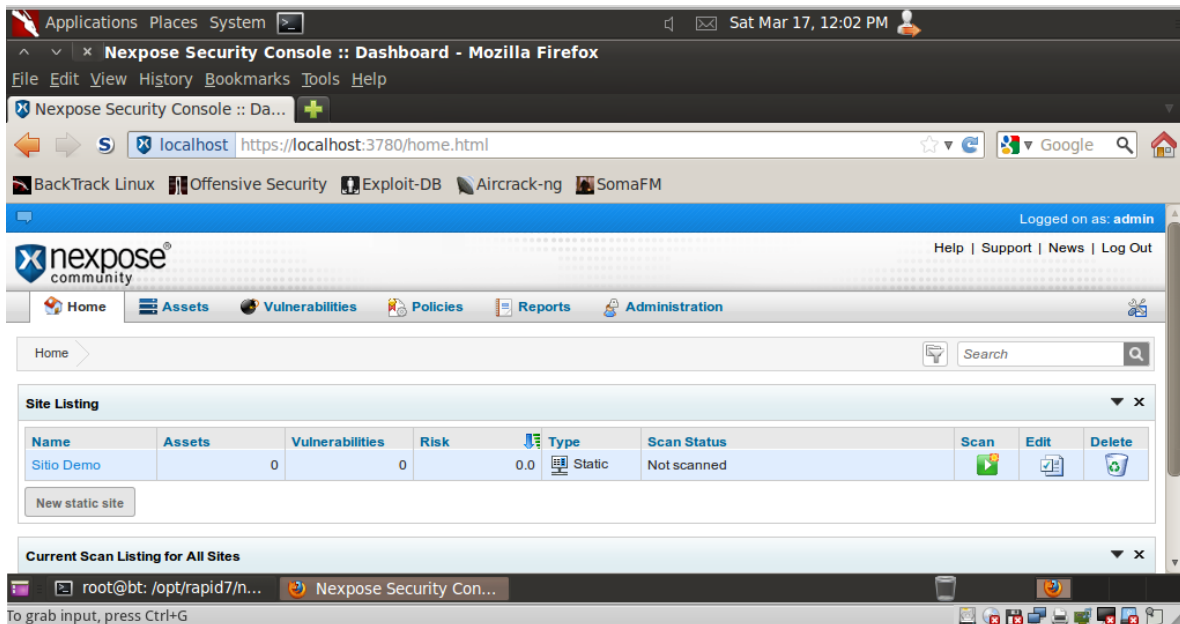
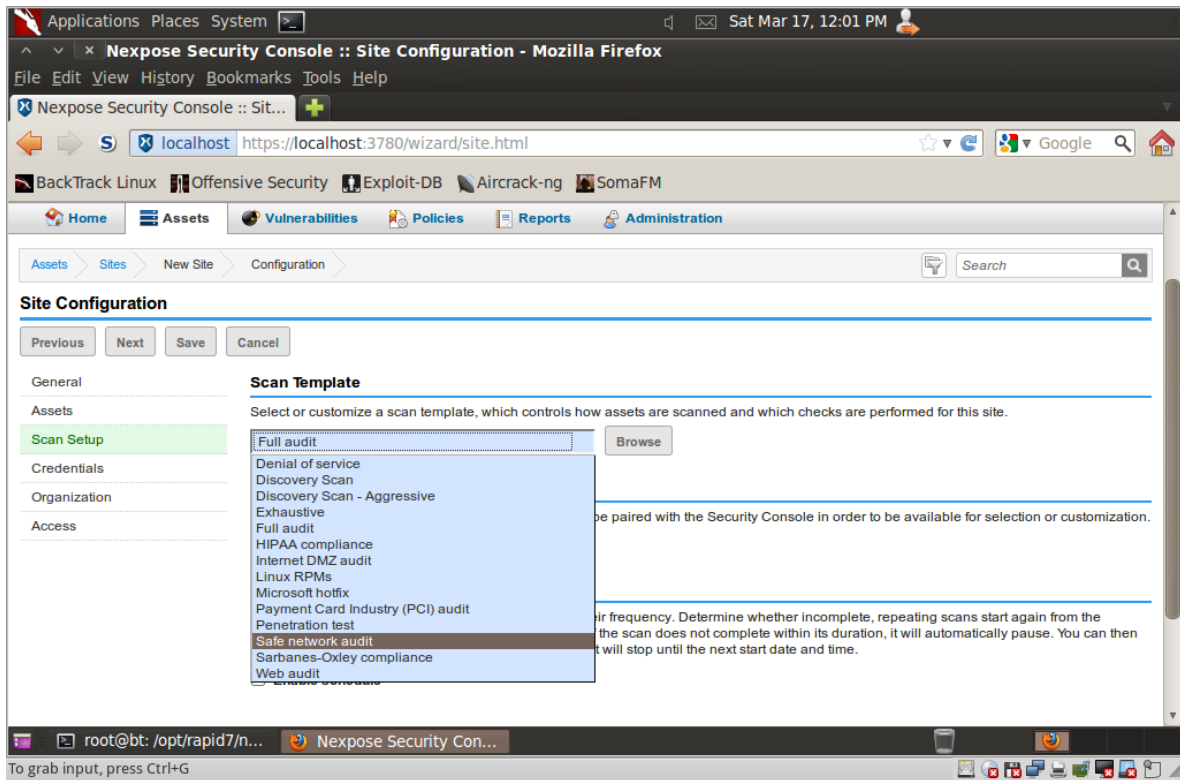
```

Ahora debería estar listo para escanear. Apunte su browser a <https://localhost:3780> e ingrese las credenciales que creó durante la instalación.

Una vez en Nexpose procederemos a crear un sitio y a definir activos (assets), escogeremos el tipo de escaneo e iniciaremos el proceso. Los activos son los equipos a analizar (IP's o nombre dns).







Luego grabamos nuestro sitio (opción Save) e iniciamos el escaneo (botón Scan).

La interfaz de Nexpose es fácil de usar y se pueden generar reportes en distintos formatos.

Pruebe a escanear la máquina de su compañero o una de sus máquinas virtuales.