

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 <u>http://www.rapid7.com/products/nexpose-community-edition.jsp</u>, 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:





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 Termin	al Help		
AutoScan files bootsplash firefox root@bt:/opt# cd rap root@bt:/opt/rapid7# nexpose	metasploit ptk nessus rapid7 id7 ls	unetbootin / web 	
<pre>root@bt:/opt/rapid7#</pre>	cd nexpose/		
eula_en.txt _j icon.ico no installer.policy ns root@bt:/opt/rapid7/	vm1.6.0_25 nse hup.out plugins c shared nexpose# cd nsc	stderr.txt stdout.txt thirdpartynotices	update.log updates .txt
root@bt:/opt/rapid7/	nexpose/nsc# ls	ncc bak	FACOULTOPS
bootstrap.txt	keystores	nsc.log	solns, bak
checks.bak	lib	nsc.sh	sal.log
checksfmwk.bak 🗾	Licenses 7	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	
<pre>root@bt:/opt# cd rap root@bt:/opt/rapid7# nexpose root@bt:/opt/rapid7# root@bt:/opt/rapid7/ eula_en.txt _j icon.ico no installer.policy ns root@bt:/opt/rapid7/ bin bootstrap.txt checks.bak checksfmwk.bak conf data db engines hs_err_pid1358.log hs_err_pid1358.log hs_err_pid21265.log root@bt:/opt/rapid7/</pre>	id7 id7 is cd nexpose/ nexpose# ls vml.6.0_25 nse hup.out plugins c shared nexpose/nsc# ls htroot keystores lib licenses logs maintenance.bak nexposeconsole.rc NeXpose.desktop NeXposeEnvironment nexpose.pid nexserv.ico nexpose/nsc# ./nsc.	stderr.txt stdout.txt thirdpartynotices nsc.bak nsc.log nsc.sh nsc.sh nse.bak nxpenv.sh nxpgsql nxplug.bak t.env nxp_sig.dbg nxshared.bak r7shared.bak	update.log updates .txt resources solns.bak sql.log temp validation.log vulns.bak webapps work

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 A Nexpose 2012-03-17T16:54:06
<pre>> JVM memory pool Code Cache (1nit = 2555904(2496K) used = 4573248(4466K) commit ted = 5111808(4992K) max = 50331648(49152K))</pre>
Nexpose 2012-03-17T16:54:06 JVM memory pool Par Eden Space (init = 6815744(6 656K) used = 16625384(16235K) committed = 17432576(17024K) max = 17432576(17024K)))
Nexpose 2012-03-17T16:54:06 JVM memory pool Par Survivor Space (init = 78643
2(/68K) Used = 265952(259K) committed = 2162688(2112K) max = 2162688(2112K))
3952K) used = 707899136(691307K) committed = 1774329856(1732744K) max = 19474677
76(1901824K))
Nexpose 2012-03-17T16:54:06 JVM memory pool CMS Perm Gen (init = 21757952(21
248K) used = 45838480(44764K) committed = 74129408(72392K) max = 167772160(16384 0K))
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 G
B 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 <u>https://localhost:3780</u> 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).

Applications Places System	2	4	🖂 Sat Mar 17, 11:57 AM	и 💄
∧ ∨ × Log on to Nexpose ·	Mozilla Firefox			
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmark	cs <u>T</u> ools <u>H</u> elp			
🛿 Log on to Nexpose	+			▼
S S localhost https	://localhost:3780/login.htm	ml		🗇 🛯 🛃 🛛 Google 🔍 🏫
BackTrack Linux MOffensive S	ecurity 🔝 Exploit-DB 🐧	Aircrack-ng 🔣 SomaFM		
X nexpose [®]				Help Support
Community				
	Log on			
	User name			
	admin			
	Password			
	•••••			
	🛱 Log on			
📷 🛛 🔄 root@bt: /opt/rapid7/n	ಲ Log on to Nexpose -	Log on to Nexpose - Mozilla	Firefox	
To grab input, press Ctrl+G				🖾 🔞 🔀 🚅 🗮 🌆 🖆 🖌



	Guatam E				C-11-17-00-			
Applications Places	System N				Sat Mar 17, 12:0	0 PM 🍝		
∧ ∨ × Nexpose Se	curity Console :: 9	ite Configura	tion - Mozilla	a Firefox				
<u>File Edit View History</u>	<u>B</u> ookmarks <u>T</u> ools <u>H</u>	elp						
Nexpose Security Cons	ole :: Sit							∇
🖕 🇼 S 🛿 localh	ost https://localhost	3780/wizard/sit	e.html			☆ ▼ 🥰	🚼 ▼ Google	۹ 🏠
BackTrack Linux 👖 Of	fensive Security 🚺	Exploit-DB 📡	Aircrack-ng 📗	SomaFM				
community								· · · · · · · · · · · · · · · · · · ·
😚 Home 📑 Assets	Vulnerabilities	Policies	Reports	🔗 Administration				
Assets Sites New Site	e Configuration					Sea Sea	rch	٩
Site Configuration								
Previous Next Save	Cancel							
General	A site is a collection	n of assets to be so	canned. Basic site	e configuration include	es selecting a Scan E	Engine and a scan tem	plate and providing	
Assets	Name	Ritia Dama						
Scan Setup	Name							
Credentials	Importance	Normal ▼						
Organization	Туре	Static						
Access	Description							
								v
📷 🛛 🖻 root@bt: /opt/rap	oid7/n 😢 Nexpo	se Security Con					U	
To grab input, press Ctrl+G						<u>e</u>	ò 🔁 🚅 😫 🛒 🖣	s 🔓 🗂 🖌





Applications Places Sys Applications Places Sys Nexpose Security Nexpose Security Console	item ≥_ ity Console :: Site Configuration - kmarks ⊥ools <u>H</u> elp <mark>:: Sit </mark>	d 🖂 Sat Mar 17, 12:01 PM 🤱 🛛 🛛 🖉
🖕 🗼 S 🔇 localhost	https://localhost:3780/wizard/site.html	्रे 🖲 🖉 Google 🔍 🏠
BackTrack Linux 👖 Offen:	sive Security 🛄 Exploit-DB 📡 Aircracl	c-ng SomaFM
Mome Assets	Vulnerabilities Dolicies	ports 🖉 Administration
Assets Sites New Site	Configuration	Search Q
Site Configuration		
Previous Next Save General	Cancel Scan Template	
Assets	Select or customize a scan template, which co	ntrols how assets are scanned and which checks are performed for this site.
Scan Setup	Full audit	Browse
Credentials	Denial of service Discovery Scan	
Organization	Discovery Scan - Aggressive Exhaustive	be paired with the Security Console in order to be available for selection or customization.
Access	Full audit HIPAA compliance Internet DMZ audit Linux RPMs Microsoft hoffix	
	Papertration test Penetration test Safe network audit Sarbanes-Oxley compliance Web audit	ir frequency. Determine whether incomplete, repeating scans start again from the the scan does not complete within its duration, it will automatically pause. You can then t will stop until the next start date and time.
🖬 🗈 root@bt: /opt/rapid7	/n 😢 Nexpose Security Con	
To grab input, press Ctrl+G		🖾 G 🖬 🚅 🗟 📽 🗖 🛆 🖉
Applications Places Sys	tem >_	් 🖂 Sat Mar 17, 12:02 PM 💄
∧ ∨ × Nexpose Secur	ity Console :: Dashboard - Mozilla	Firefox
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> oo	kmarks <u>T</u> ools <u>H</u> elp	
🛿 Nexpose Security Console	:: Da 🕂	v

Inexpos	se°					Help Supp	Logged on as: adm ort News Log Ou
Mome	📑 Assets 🛛 💣 Vu	Inerabilities 🚯	Policies 📃 Reg	oorts 🔗 A	dministration		æ
Home						Search	٩
Site Listing							▼ ×
	Assets	Vulnerabilities	Risk	Туре	Scan Status	Scan	Edit Delete
lame				III Static	Notecanned		
Name Sitio Demo	0	0	0.0		Not scanned		
Name Sitio Demo New static site	0	0	0.0		Notacalificu		

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.