Buscando Vulnerabilidades en Windows: Tenable Nessus

Su sistema experimenta una lentitud inexplicable? Instaló la última versión de antivirus y aún así sigue lento? En ese caso es probable que su sistema sea víctima de un *cracker* que aprovechando un *exploit* en su sistema, está usando los recursos de su computadora y la ha convertido en un *botnet* o *zombie*.

Antes de continuar definamos los términos técnicos (si este punto está claro, por favor salte esta sección):

- **Cracker:** individuo que hace uso de herramientas tecnológicas y se vale de las vulnerabilidades presentes en un sistema para penetrar en él sin permiso y realizar actividades maliciosas como robar claves, números de tarjetas de crédito, o usar el sistema para desde ahí ejecutar daños a un tercero. Al cracker también se lo conoce como "*hacker de sombrero negro*".
- **Exploit:** es una vulnerabilidad presente en un sistema de cómputo producto de una mala programación en el sistema operativo, o en alguna aplicación o servicio y que puede ser aprovechada por un cracker para efectuar un ataque que puede ser de acceso (es decir para ingresar al sistema) o de denegación de servicio (causar que el sistema o la aplicación/servicio dejen de funcionar).
- **Botnet/Zombie:** es un sistema de cómputo en el cual un cracker ha logrado penetrar ilegalmente y ha instalado *malware* sin conocimiento del usuario, el cual le permite controlar el equipo a control remoto y enviarle órdenes ya sea para extraer información del usuario local o bien para realizar ataques hacia un tercero (como por ejemplo enviar *spam* o realizar ataques de denegación de servicio).
- **Spam:**
- **Malware/Spyware:** software malintencionado que se instala sin conocimiento del usuario en un sistema.

Herramientas para detección de vulnerabilidades

Si tiene dudas acerca de si su sistema está libre de vulnerabilidades que puedan ser explotadas, entonces hay algunas acciones sencillas que puede ejecutar por su cuenta antes de llamar a su consultor de seguridad de confianza:

1. Actualizar su equipo con los últimos parches.
   1.1. En Windows puede hacerlo desde el Panel de Control en la opción de Actualizaciones Automáticas (Microsoft Update).
   1.2. En otros sistemas operativos usualmente hay una opción similar que permite descargar actualizaciones desde el sitio web del fabricante.
2. Instalar un software que detecte y remueva *malware*, además de un buen software de antivirus. Ej: Windows Defender, Malicious Software Removal Tool, Eset Nod32 Antivirus/Antispyware, Cisco Security Agent, etc.

3. Configurar un firewall de host que impida las conexiones no autorizadas hacia nuestro equipo. En Windows podemos usar el firewall que viene integrado con el sistema y en Linux/Unix podemos hacer uso de herramientas de firewall muy buenas y de código abierto como IPTables o IPFilter.
4. Ejecutar una herramienta básica de detección de vulnerabilidades: Nmap, Tenable Nessus, Metasploit, etc.

En este artículo nos vamos a concentrar en la opción 4 y la herramienta que vamos a utilizar es Tenable Nessus.

Análisis de vulnerabilidades con Tenable Nessus

Tenable Network Security es una empresa norteamericana muy reconocida en el medio de seguridad de información, que se dedica a desarrollar software para detectar vulnerabilidades, monitoreo de equipos en tiempo real, análisis de logs, entre otras maravillas. Su producto estrella es el **Tenable Security Center**, el cual permite realizar de forma centralizada:

- Descubrimiento de activos de redes
- Escaneo de vulnerabilidades distribuido
- Configuraciones de políticas de auditoría
- Agregación y correlación de logs
- Control del flujo de acciones de los administradores

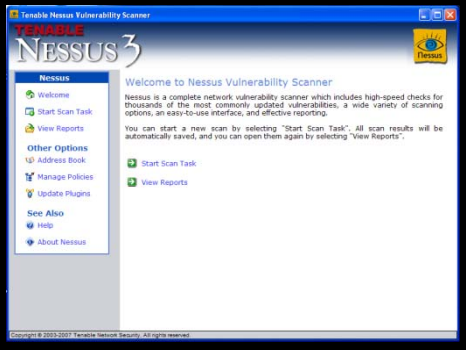
Debido a la diversidad de opciones y facilidad de uso de la interfaz gráfica que ofrece este software para descongestionar la ardua tarea de los Administradores de Seguridades de Redes y Seguridades, sólo está disponible en versión comercial y tiene un costo de licenciamiento a partir de 500 ip's.[i]

Sin embargo existe una opción de software más sencilla que solamente realiza chequeo de vulnerabilidades de equipos individuales, llamada **Nessus**[1]. Este software se puede descargar **gratuitamente** desde este enlace: http://www.tenablesecurity.com/download/. La única condición para hacerse acreedor a la licencia es aceptar un acuerdo y comprometerse a utilizarlo de modo personal, no comercial. Nessus está disponible para Windows, Linux, MacOS y FreeBSD.

A pesar de su sencillez y facilidad de uso, Nessus es un software muy eficiente en la detección de vulnerabilidades y Tenable invierte mucho esfuerzo en investigación y desarrollo para proveer plug-ins actualizados para detectar las nuevas vulnerabilidades, conforme son descubiertas.

Para la realización de nuestro pequeño laboratorio vamos a asumir que usted ya descargó, instaló y actualizó Nessus con los últimos plug-ins.

Ejecutando Nessus



La interfaz de Nessus es fácil de utilizar como puede observarse en la figura.

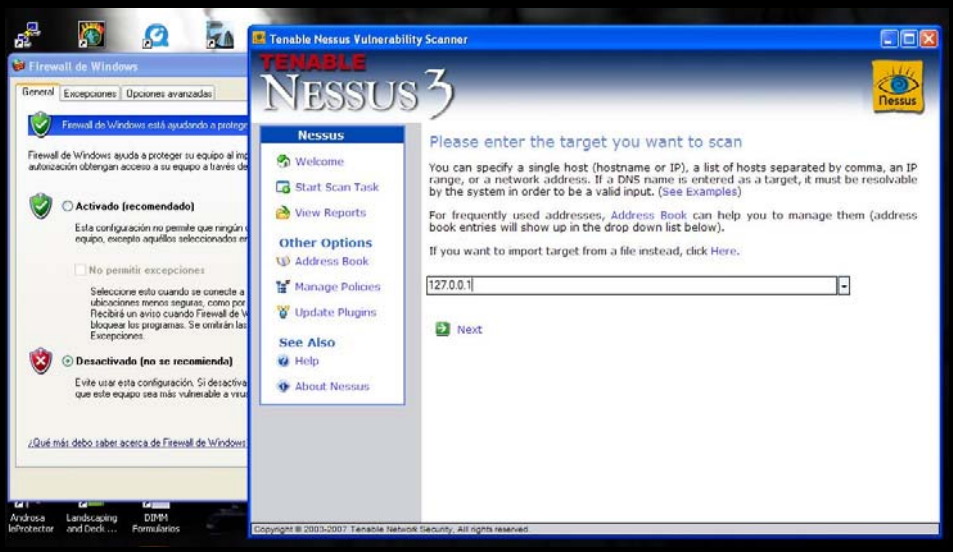
Para nuestro laboratorio vamos a escoger la opción "Start Scan Task" haciendo click en el botón respectivo.

Esto nos conducirá a una segunda pantalla en donde se nos pide ingresar el *target* que deseamos escanear, es decir el equipo sobre el cual vamos a realizar el chequeo de vulnerabilidades. Deberemos ingresar la dirección IP del

[1] Si desea ver un video demostrativo de Nessus revise este url: http://www.elixircorp.biz/videos.html

equipo. El equipo a analizar debe estar en una red alcanzable desde nuestra red local.

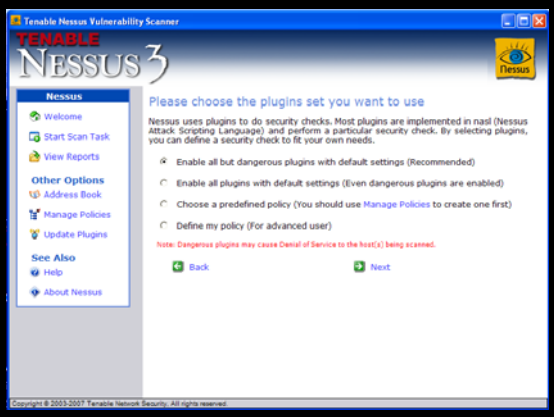
Para este ejemplo vamos a hacer la prueba con el mismo equipo donde instalamos Nessus, que en nuestro caso es una laptop Toshiba con Windows XP Service Pack 3 y a propósito vamos a detener el servicio de Firewall de Windows para que Nessus pueda detectar todas las vulnerabilidades, inclusive las que permanezcan ocultas detrás del Firewall. Dado que el equipo que vamos a escanear es nuestro propio host, entonces la dirección del target es la IP de Loopback: 127.0.0.1

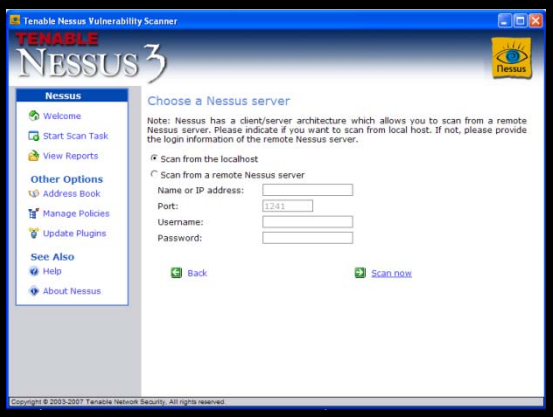


En la siguiente pantalla Nessus nos consulta el tipo de escaneo que deseamos hacer y nos ofrece cuatro opciones:

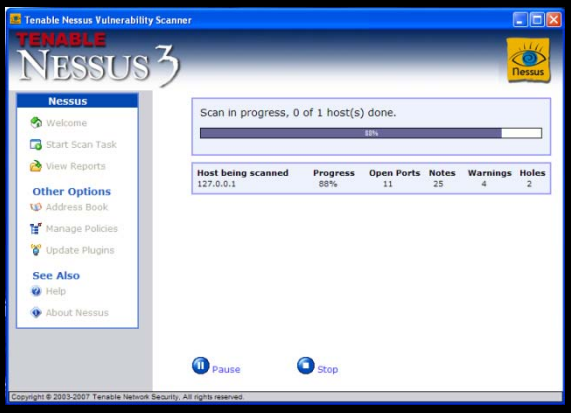
1. *Enable all but dangerous plugins with default settings*
   1.1. Esta es la opción por defecto y habilita el chequeo de todas las vulnerabilidades y exploits presentes en la base de datos de Nessus (plug-ins), a excepción de aquellos que puedan realizar un posible daño en el sistema escaneado, como por ejemplo: detener un servicio, reiniciar el equipo, provocar una caída del sistema, etc.
2. *Enable all plugins with default settings*
   2.1. Esta opción habilita todos los chequeos incluyendo aquellos que podrían causar daños en el equipo analizado. Si el administrador quiere estar seguro que su equipo está protegido contra todo, esta debería ser la opción elegida; pero en este caso lo recomendable sería realizar el chequeo fuera de horas laborables y luego de haber realizado un respaldo completo del sistema evaluado.
3. *Choose a predefined policy*
   3.1. En este caso podemos seleccionar una política personalizada de chequeo de vulnerabilidades que hayamos definido previamente a través del menú de manejo de políticas (Manage Policies).
4. Define my policy
   4.1. este escaneo en particular y aplicarla al sistema que analicemos.

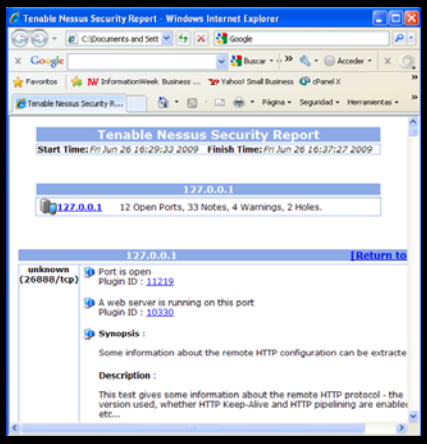
Una vez seleccionada la opción de escaneo Nessus nos pregunta desde dónde vamos a realizarlo, si desde nuestro equipo local o si desde un servidor remoto Nessus. En nuestro caso lo haremos desde nuestro mismo equipo (*Scan from the localhost*).





Finalmente procedemos a realizar el escaneo de vulnerabilidades, lo cual es tan fácil como hacer click en *Scan Now* y dejar que Nessus se encargue de ejecutar pruebas contra nuestro equipo.





Al terminar el escaneo Nessus genera un Reporte de Seguridad en formato html, el cual se visualiza automáticamente en nuestro navegador de Internet. El reporte que genera Nessus es muy detallado e incluye una descripción de todas las vulnerabilidades detectadas, con el nivel de severidad y una explicación de cómo afecta esto al sistema, además incluye enlaces externos a sitios tanto de Tenable como de terceras partes en donde hay información completa sobre la vulnerabilidad e inclusive cómo resolver el problema.

En resumen Nessus es una excelente herramienta para hacer diagnósticos a priori que nos permitan corregir problemas, antes someternos a una Auditoría de Seguridad Externa completa o a un Test de Intrusión.

Esperamos que este artículo les sea de utilidad, si tienen inquietudes acerca de este y otros temas relacionados por favor no duden en contactarnos.

Por Karina Astudillo B. – Gerente de IT
CCAI – CCNA – SCSA – Cisco FE SMB

[i] Para información de licenciamiento y demostraciones de Tenable Security Center por favor enviar un mail a ventas@elixircorp.biz o llamar al 593-4-5000141 ó al 593-9-9429880