Análisis de Vulnerabilidades con Nessus

Requisitos:

- Nessus 3.0 o superior.
- Windows 2000/XP.

Descripción:

Nessus es un popular analizador de vulnerabilidades, utilizado por la mayoría de los profesionales de seguridad.
Para su funcionamiento Nessus incorpora dos componentes, por un lado, el servidor, el cual será quien contenga los plugins (actualizaciones) y además será quien ejecute finalmente los escaneos, y por el otro lado, un cliente, que será quien indique las tareas a ser realizadas por el servidor. Tenga en cuenta que es muy común encontrar tanto el cliente como el servidor sobre la misma PC (tal como lo realizaremos en este laboratorio).

Instalación:

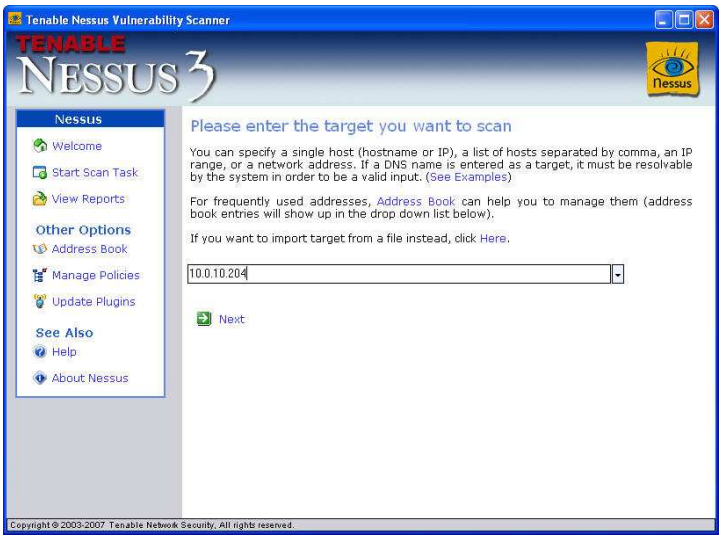
Realice la instalación por defecto de la herramienta, haciendo doble clic sobre el archivo ejecutable (Nessus-3.0.6.1). Una vez concluida la instalación, será necesaria una conexión a internet para actualizar los plugins.

Desarrollo:

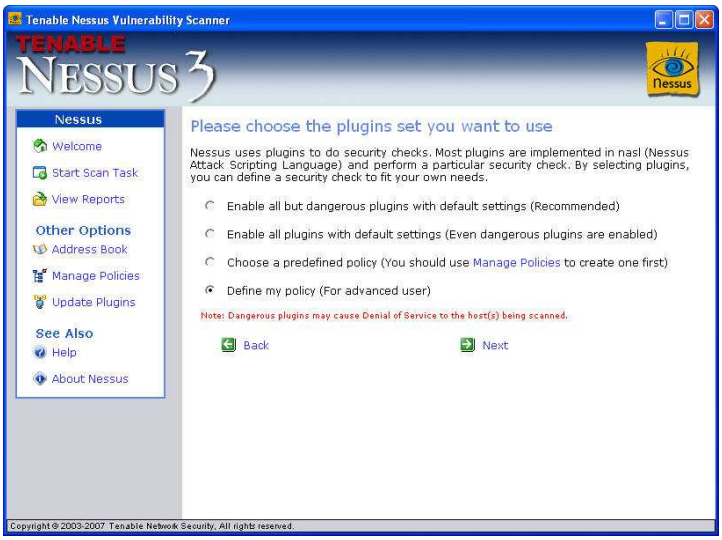
1. Inicie la aplicación haciendo doble clic sobre el ícono del escritorio "Tenable Nessus" o haga clic en "Inicio > Programas > Tenable Network Security > Nessus > Tenable Nessus".

2. Haga clic sobre "Start Scan Task".

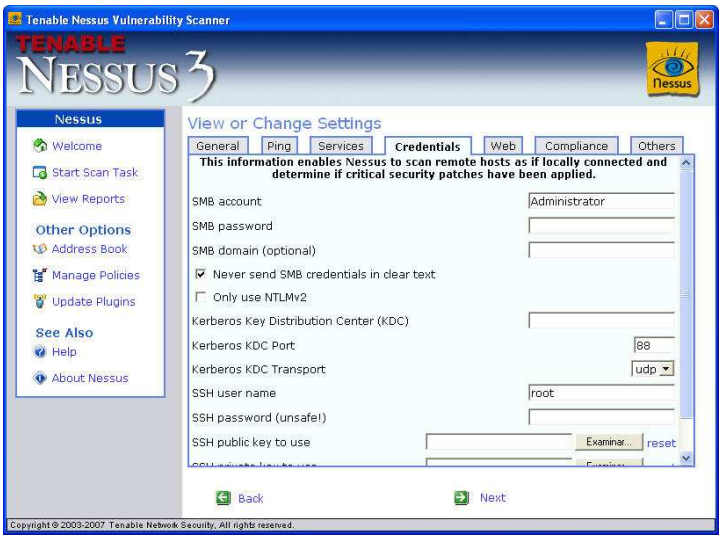
3. Complete con la dirección IP del objetivo del escaneo y a continuación haga clic en "Next".



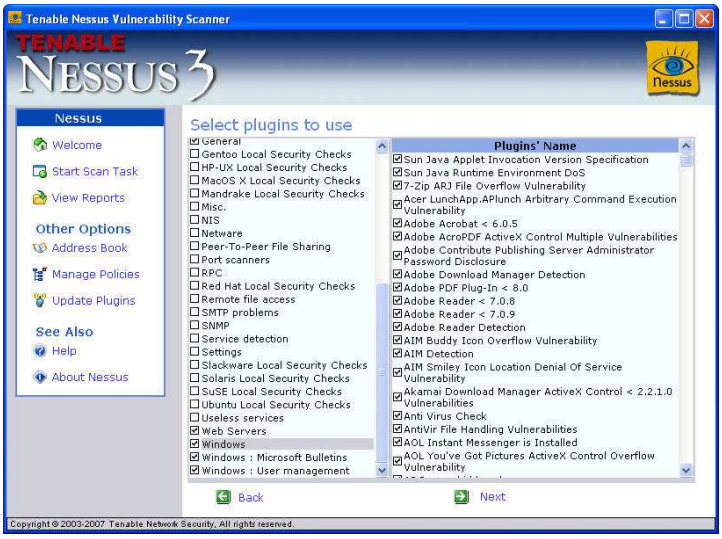
4. A continuación se le presentarán cuatro opciones que definirán la forma del escaneo. Seleccione "Define my policy" de forma de poder personalizar las opciones del escaneo y a continuación haga clic en "Next".



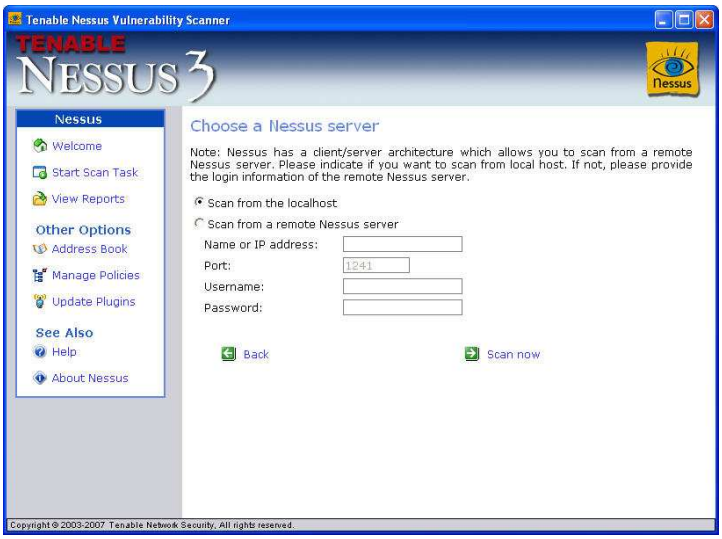
5. Revise las opciones disponibles para el escaneo sobre cada una de las solapas. Puntualmente haga clic sobre la solapa "Credentials" y verifique que ningún usuario figure sobre el campo "SMB account", haga lo mismo sobre el campo "SMB password". De esta forma, el análisis se llevará a cabo sin ningún tipo de credenciales particulares. Al finalizar, haga clic en "Next".



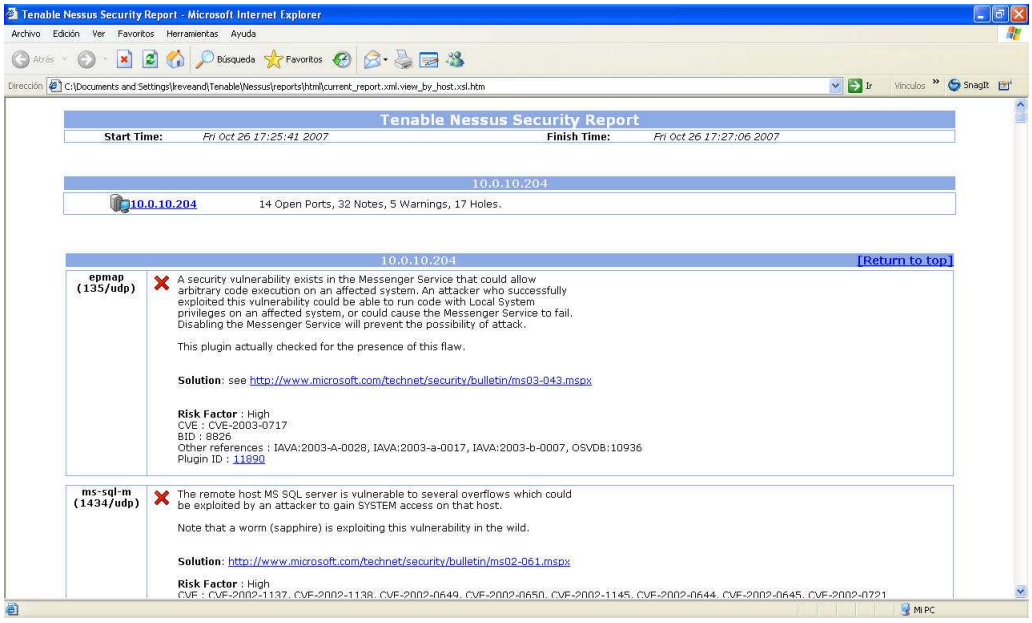
6. En el siguiente paso podremos seleccionar qué tipo de escaneos realizar a través de la selección de los plugins a utilizar. Esto nos permitirá disminuir la cantidad de pruebas que se llevarán a cabo durante el escaneo, disminuyendo la duración del mismo. Seleccione solamente los plugins relacionados con sistemas Windows y los servicios que éste brinda (Ej.: Windows, Web Servers, Generals, Databases, etc.). A continuación haga clic en "Next".



7. La siguiente ventana nos pide que seleccionemos un Server Nessus. Debido que se utilizará el server de nuestra propia PC, seleccione "Scan from the localhost" y haga clic en "Scan now".



8. Una vez concluido el análisis, se le presentará un informe a través del browser. Revise la información obtenida.



9. Realice un nuevo escaneo, pero esta vez incluyendo las credenciales del administrador y verifique la información obtenida. ¿Es similar a la obtenida en el primer escaneo?