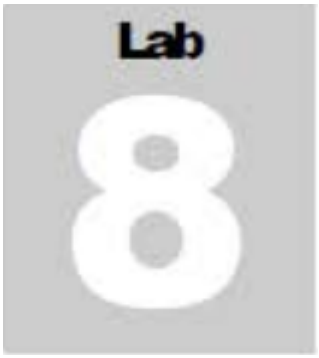


Análisis de vulnerabilidad usando el Nessus.

Nessus le permite auditar una red de forma remota y determinar si ha sido interrumpida o mal utilizada de alguna manera. También proporciona la capacidad de auditar localmente una máquina específica para detectar vulnerabilidades.

Objetivos del laboratorio

Este laboratorio le brindará experiencia en tiempo real con el uso de la herramienta Nessus para buscar vulnerabilidades en la red.

Descripción general de la exploración de vulnerabilidades

El escaneo de vulnerabilidades es uno de los tipos de actividad de evaluación de seguridad que realizan los profesionales de la seguridad en su red doméstica. Les ayuda a encontrar posibles vulnerabilidades de red.

Tareas del laboratorio

1. Inicie la máquina virtual de Windows Server 2016 antes de comenzar esta práctica de laboratorio.

2. Dirijase al directorio donde tenga almacenado el ejecutable de Nessus y de doble click al archivo .exe

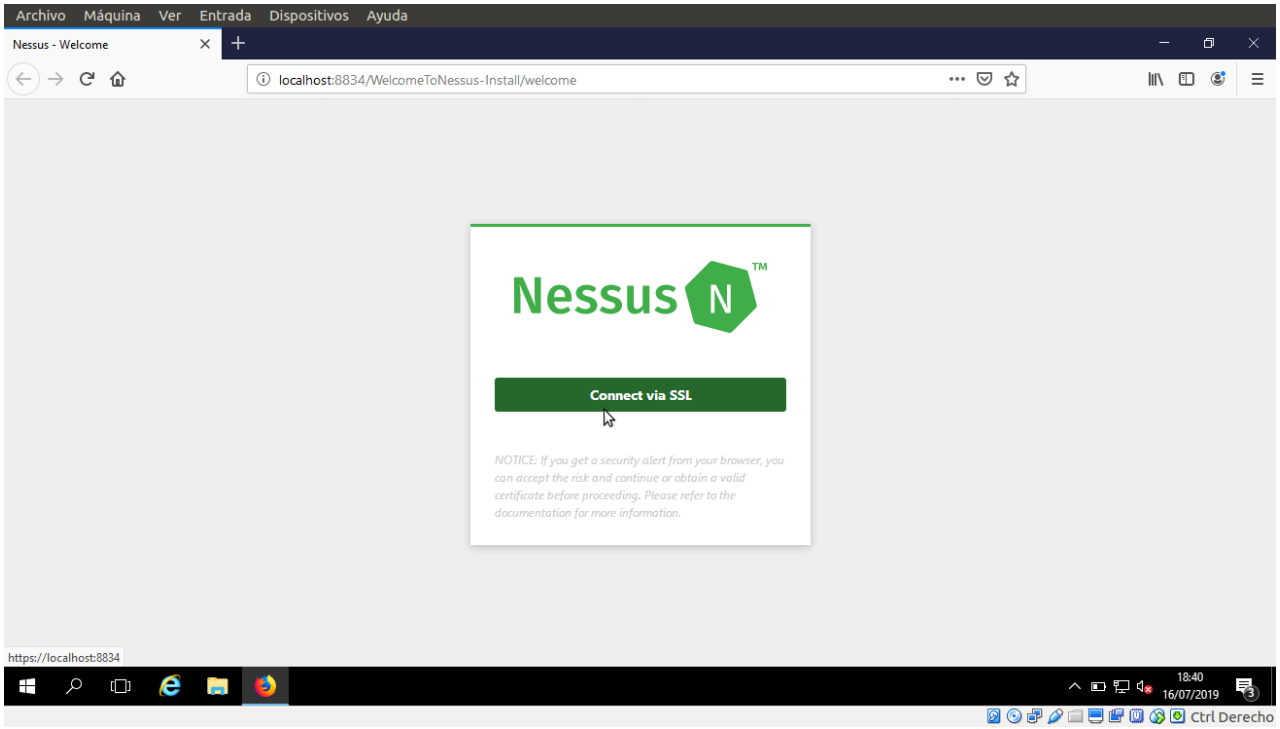
3. Si aparece la ventana emergente de advertencia de seguridad de archivo abierto, haga clic en **Ejecutar**.

4. Aparece el **Asistente de instalación de Nessus de Tenable**. Siga los pasos de instalación para instalar Nessus. Debes aceptar toda la instalación por defecto.

5. Durante la instalación, si aparece una ventana emergente del servidor de Windows, haga clic en instalar o vaya al paso siguiente

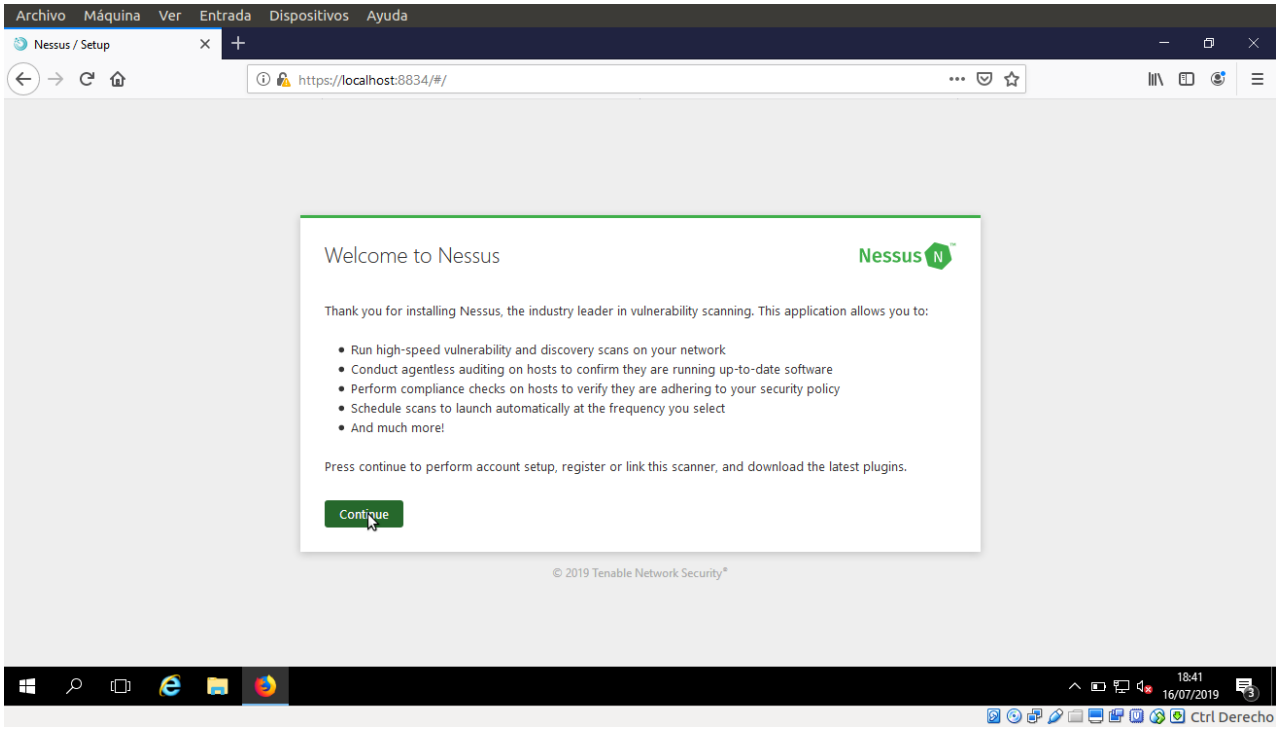
6. Después de la instalación, Nessus se abre en su navegador predeterminado.

7. Aparece la ventana **Bienvenido a Nessus**. Haga clic en el enlace **aquí** para conectarse a través de **SSL**.



8. **Certificado de seguridad del sitio no es de confianza!** Aparece en la ventana. Haga clic en **Continuar** de todos modos.

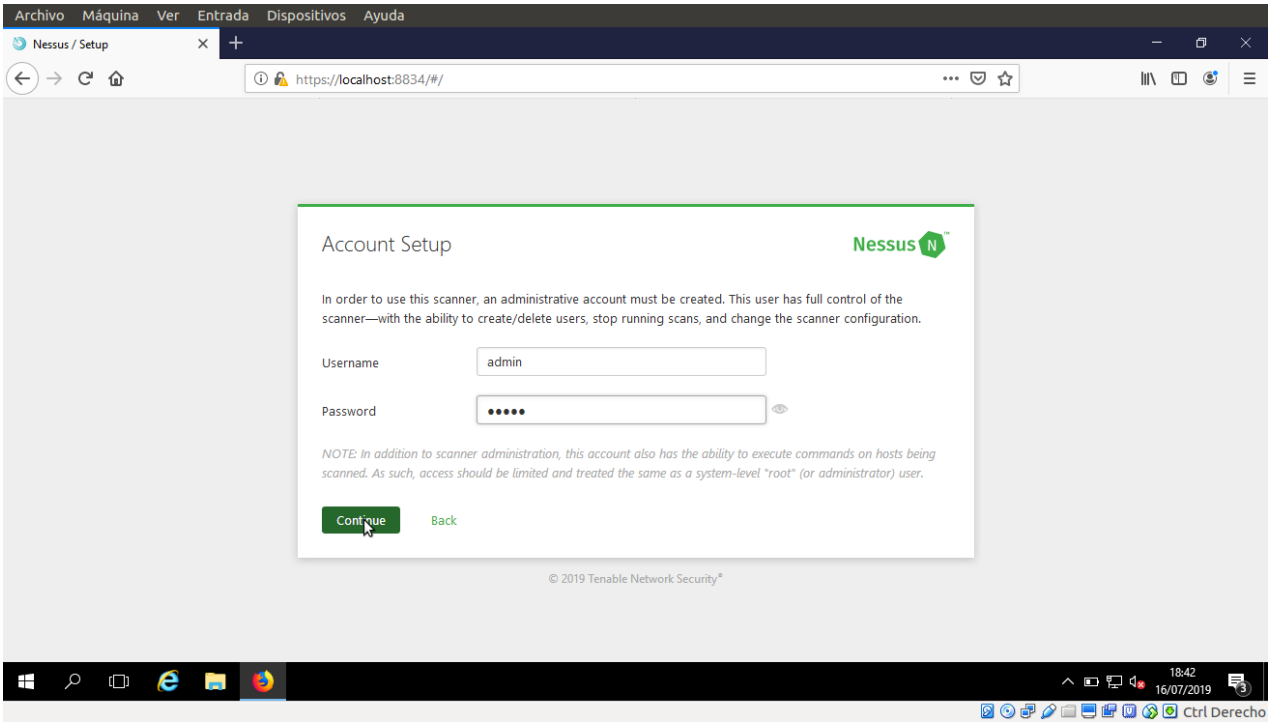
9. Aparece la ventana Bienvenido a Nessus. Haga clic en el botón **Comenzar.**



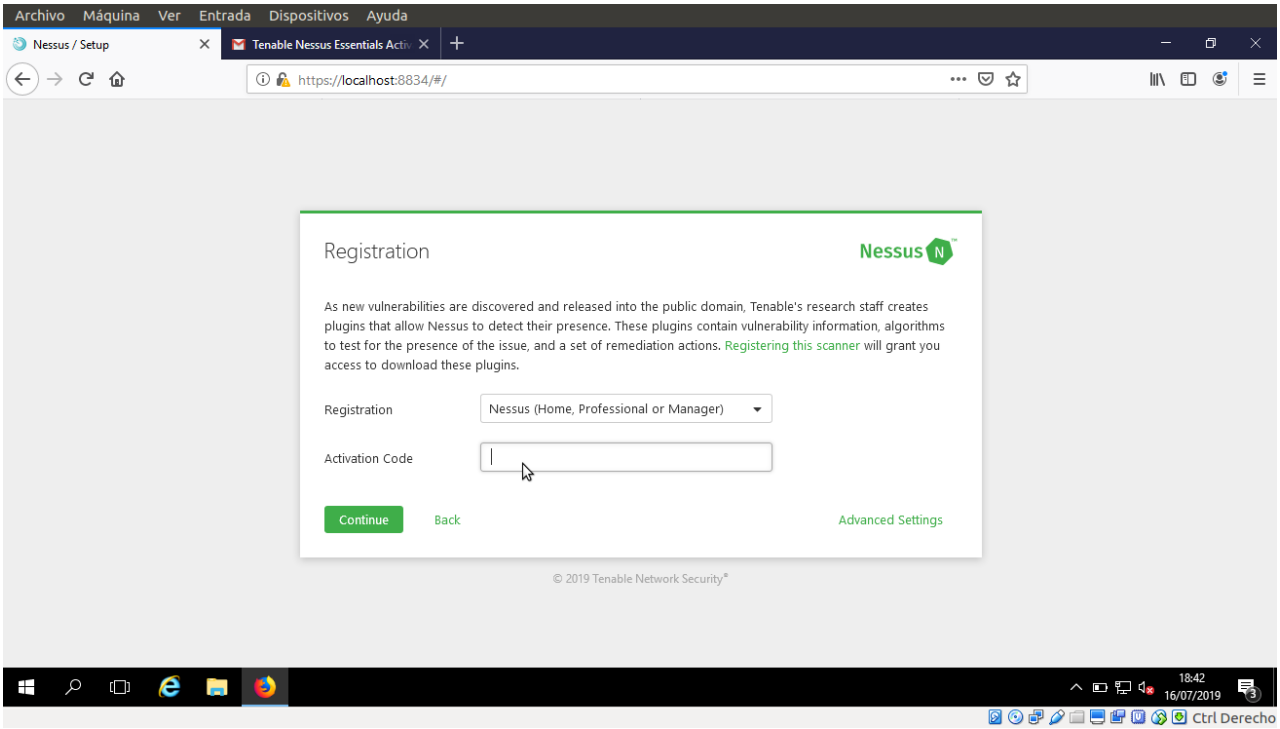
10. Aparece la ventana de configuración inicial de la cuenta.

11. Crear credenciales para usar para el control administrativo del escáner. Puede usar "admin" y "admin" aquí, luego haga clic en **Siguiente.**

12. Estas credenciales se utilizarán para iniciar sesión en Nessus en el momento de la exploración de vulnerabilidades.

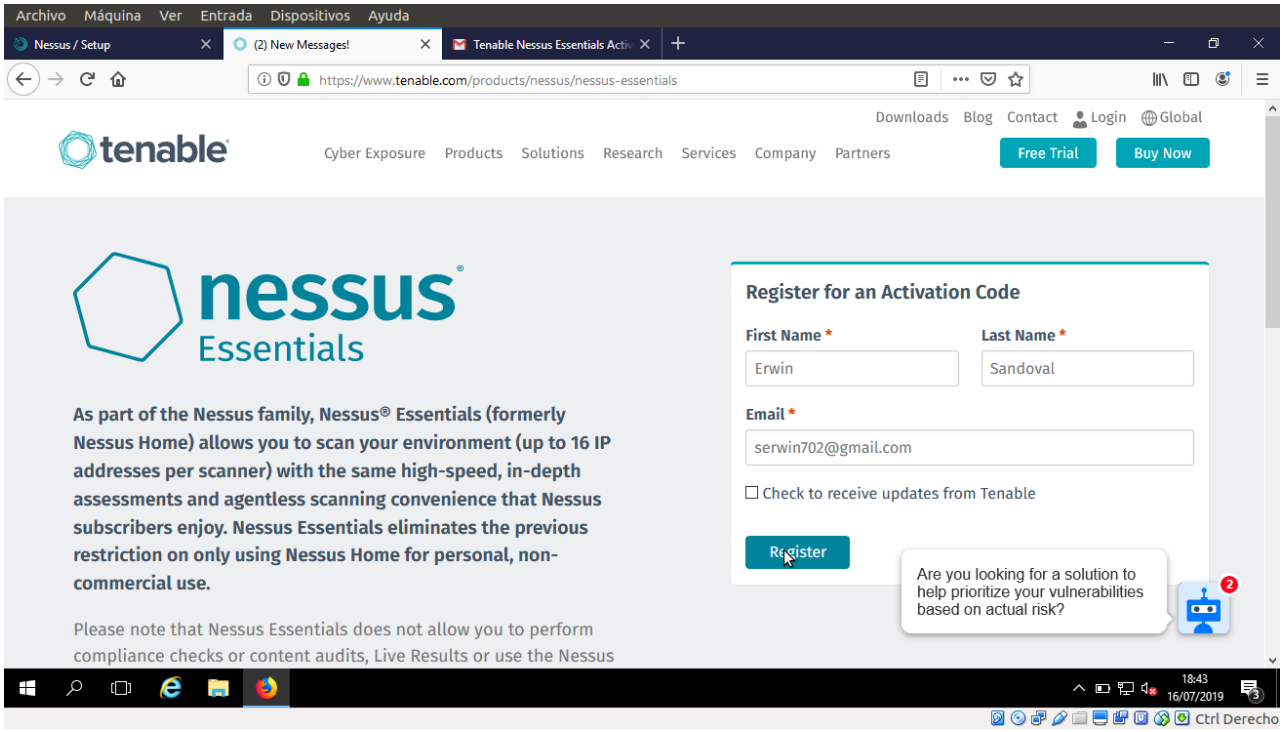


13. Aparece la ventana **Registro de alimentación de complementos**, en la que debe ingresar un código de activación. Vaya a la página web de Tenable y regístrese para obtener un código de activación. Continúa con el siguiente paso para completar el proceso.



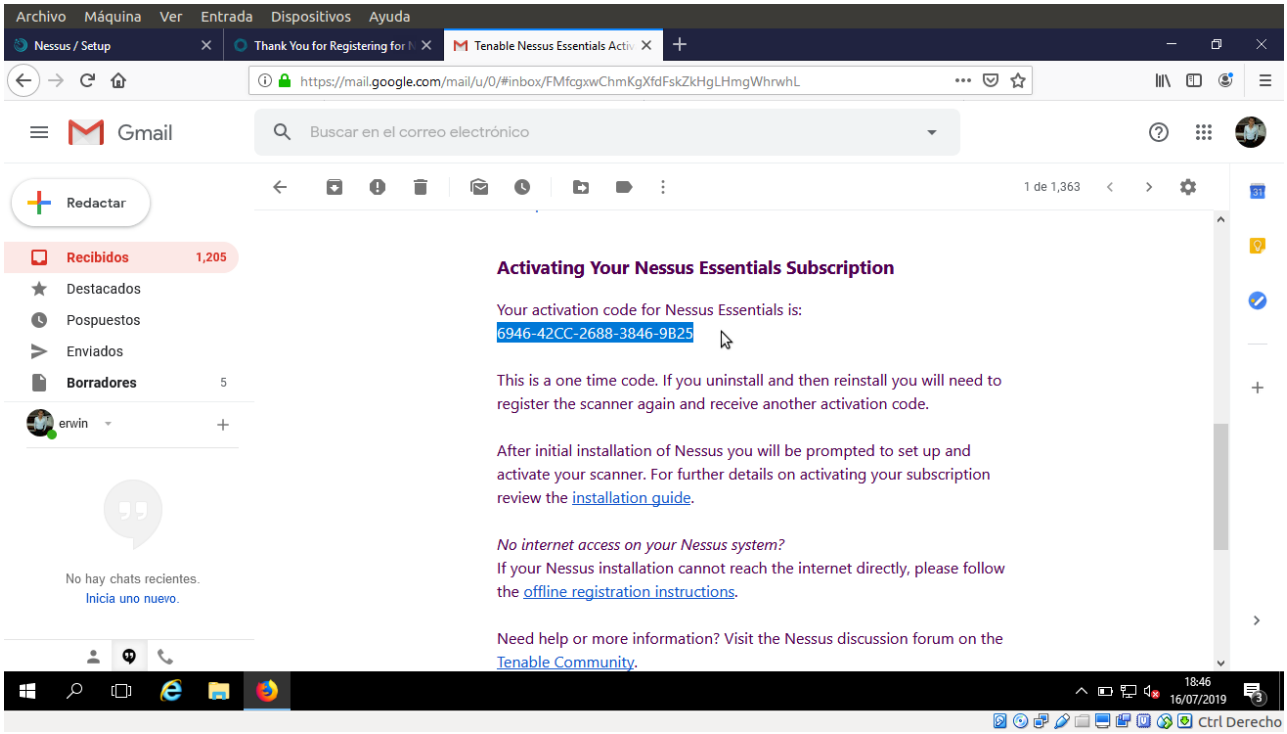
14. Abra una nueva pestaña en el navegador y escriba el enlace http://www.tenable.com/products/nessus-home en la barra de direcciones y presiona **Enter**.

15. Aparece la página de inicio de Nessus. Ingrese los detalles en **Registro para un código de activación**, acepte el acuerdo de licencia y haga clic en **Registrar**. Puede usar un alias, pero necesitará un correo electrónico válido para recuperar el código de activación. Es posible que desee considerar la creación de una cuenta de correo electrónico de alias si no tiene una.

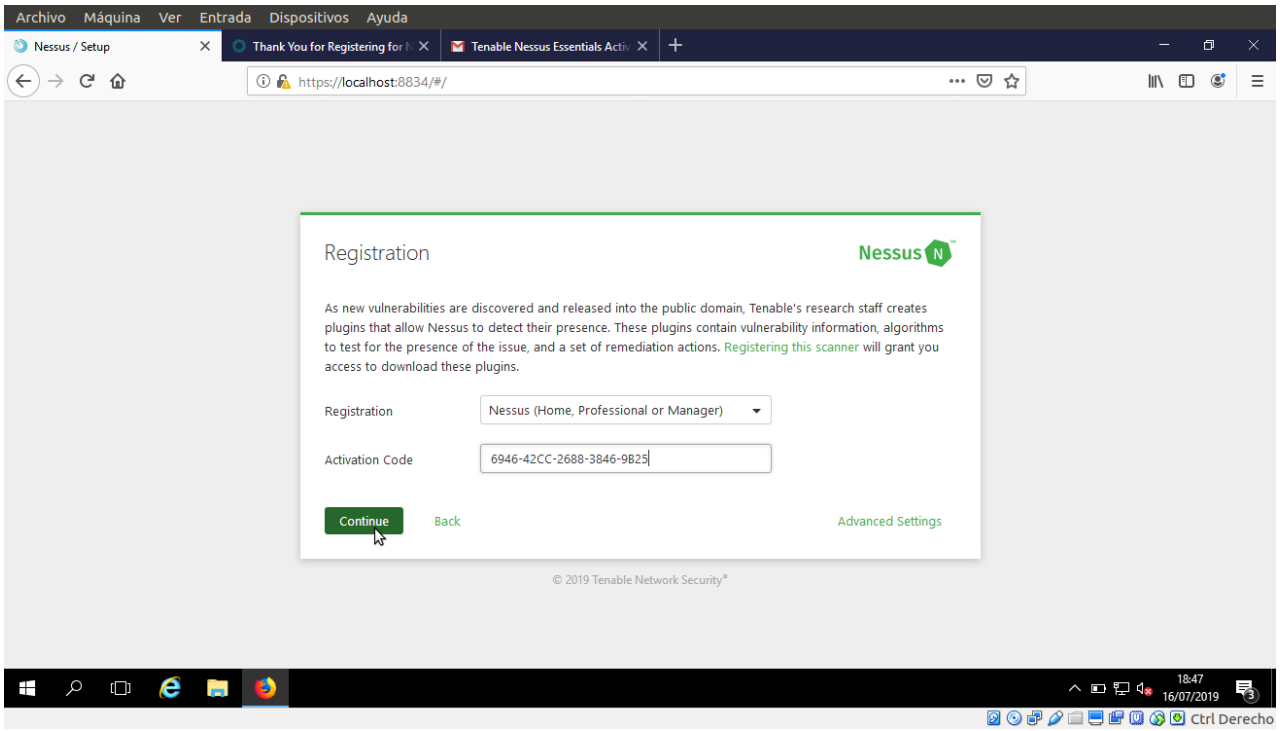


16. Una vez que hayas terminado, cierra la ventana.

17. Inicie sesión en su cuenta de correo electrónico, abra el correo de la bandeja de entrada de Tenable Nessus y copie el código de activación.



18. Cambie a la ventana **Registro de fuente de complemento** y pegue el código de activación en el campo **Introduzca el código de activación**. Haga clic en **Siguiente**.

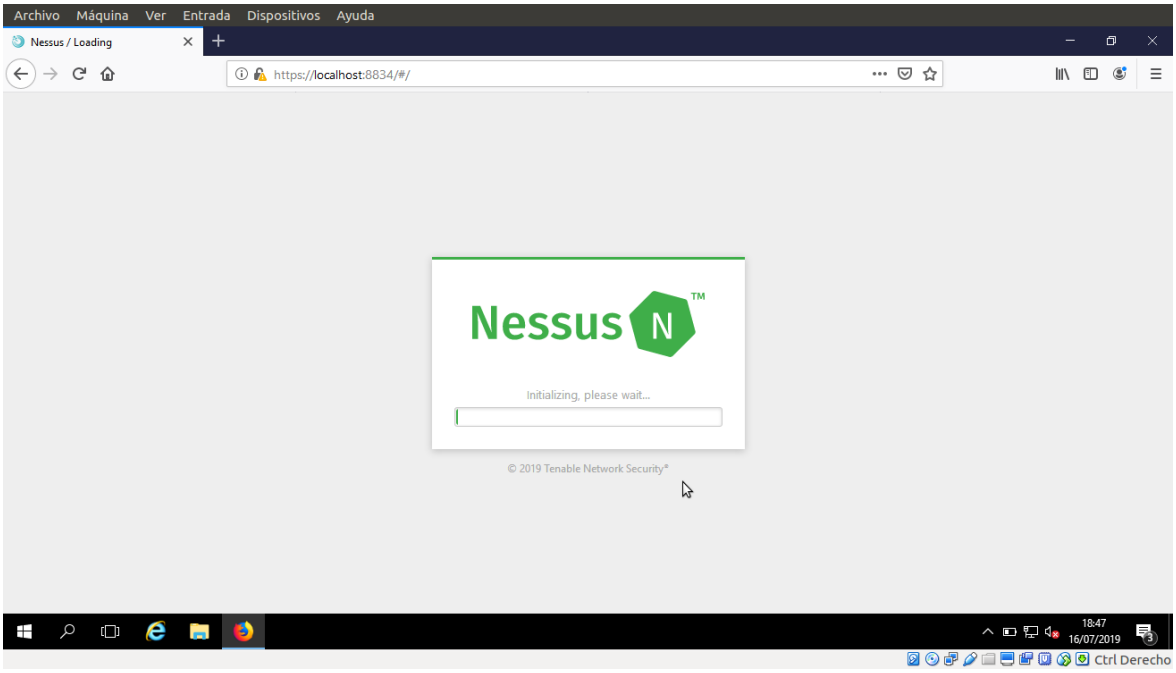


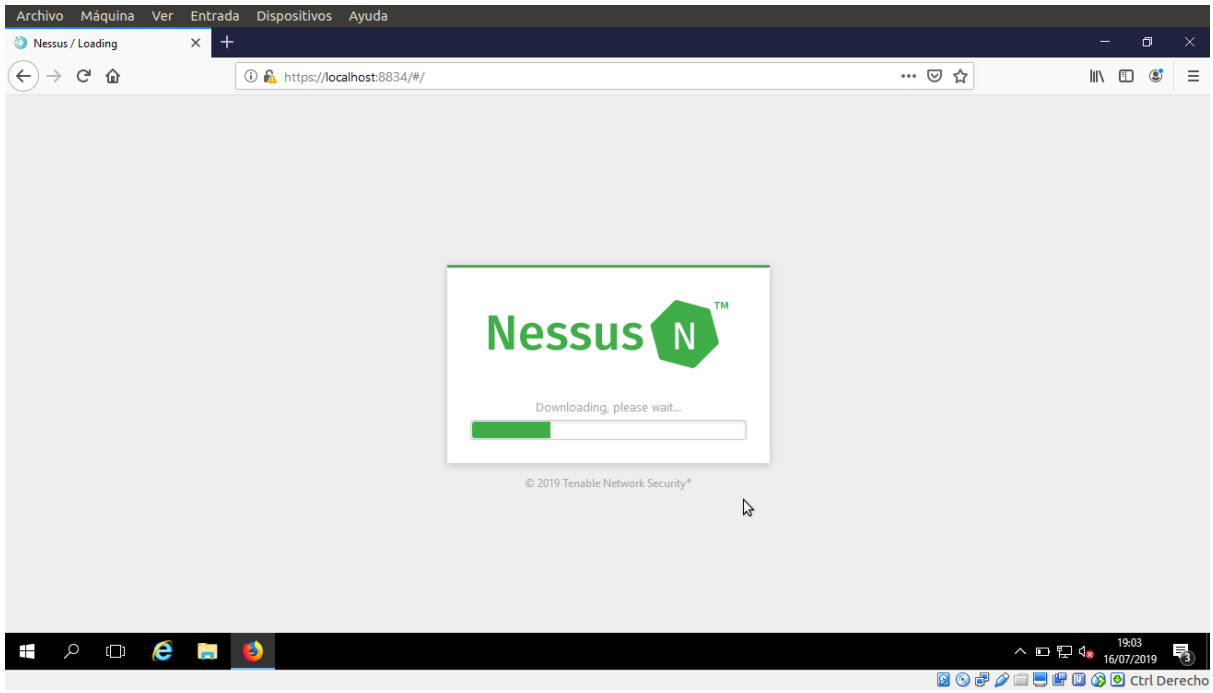
19. Aparece la ventana de **registro**

20. Espere hasta que el escáner esté registrado con **Tenable**.

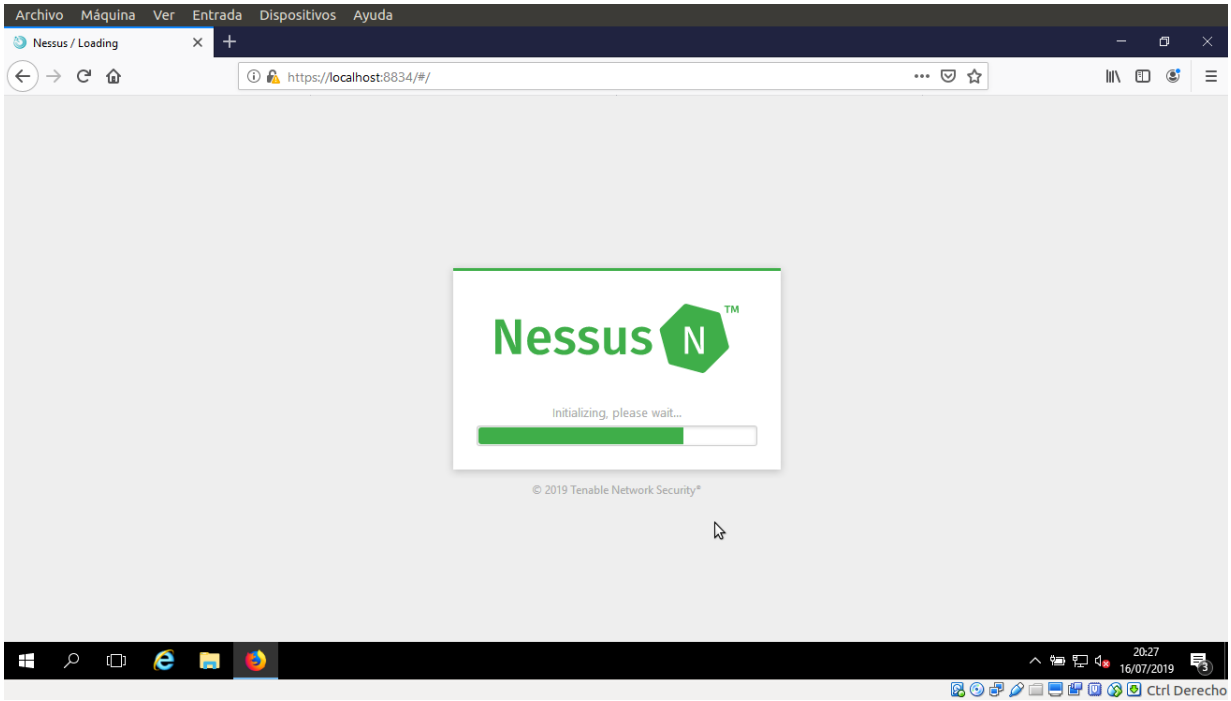
21. Después de un **registro exitoso**, haga clic en **Siguiente: Descargar complementos** para descargar complementos de Nessus.

22. Nessus comenzará a buscar los complementos y los instalará. Tendrá tiempo para instalar complementos y realizar la inicialización.

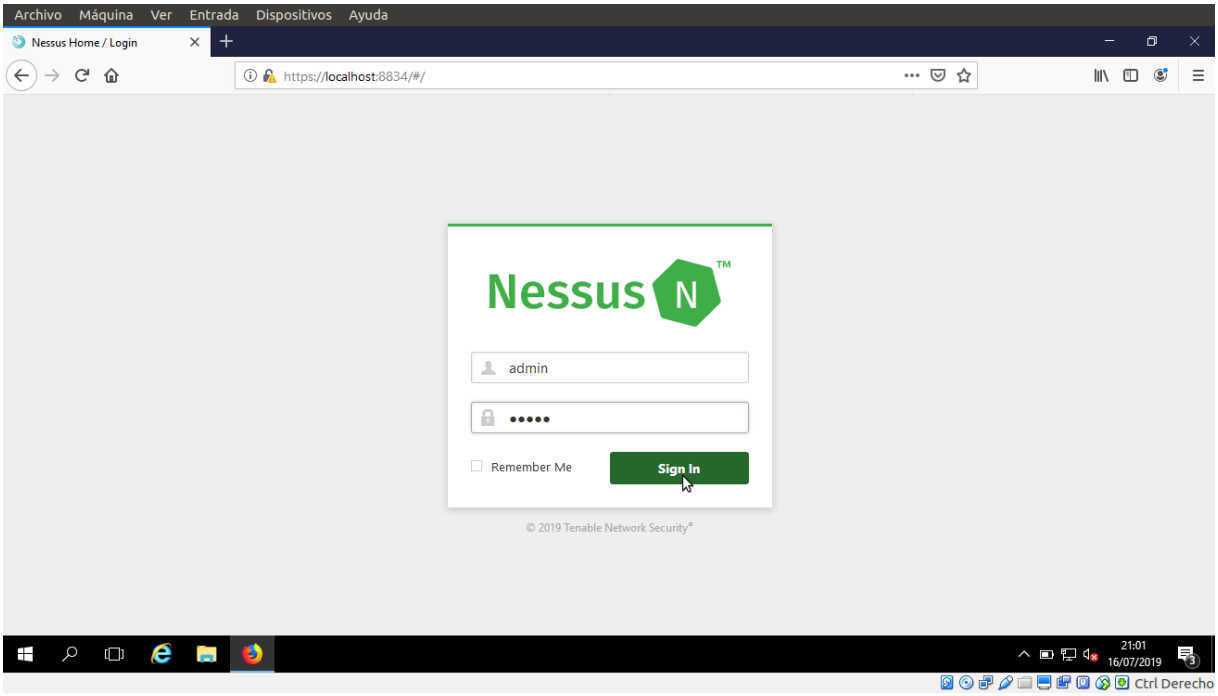




23. Una vez hecho esto con la descarga de plugins, Nessus comienza a inicializarse. A Nessus le lleva algo de tiempo inicializarse.



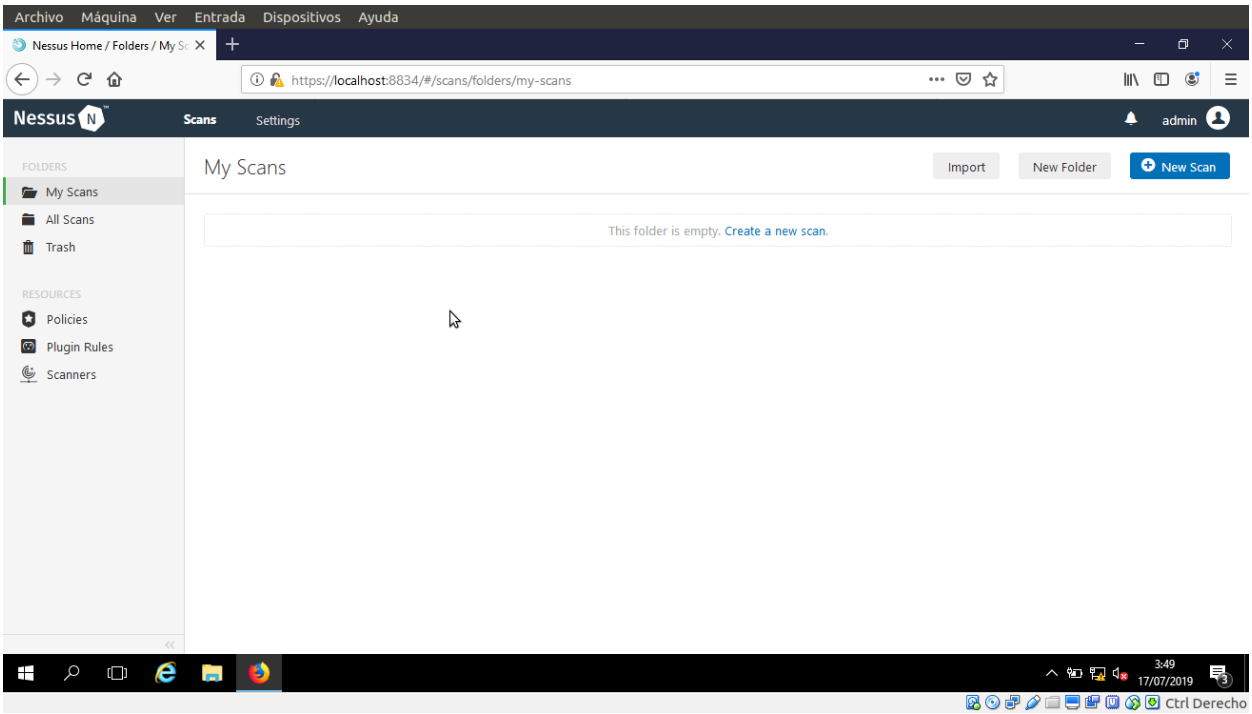
24. Al finalizar la inicialización, aparecerá la página de inicio de sesión de NESSUS.



25. Ingrese el nombre de usuario y la contraseña del paso de configuración de la cuenta inicial anterior (recomienda Usuario: admin, Contraseña: contraseña y haga clic en Iniciar sesión.

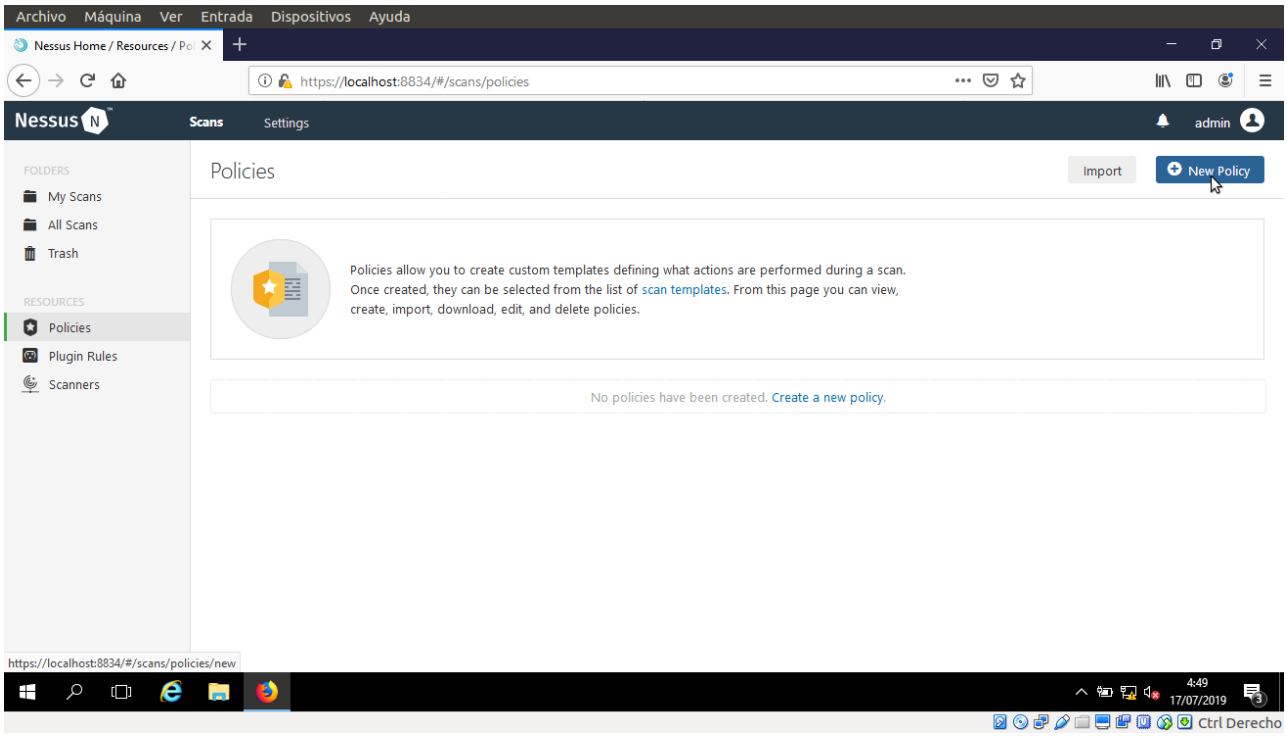
26. Después de iniciar sesión correctamente, se abrirá la ventana de Novedades de nessus sobre la ventana de inicio / escaneo de nessus. haga clic en cerrar.

27. Se abrirá la ventana nessus/scan, como se muestra en el siguiente srcrenshot.

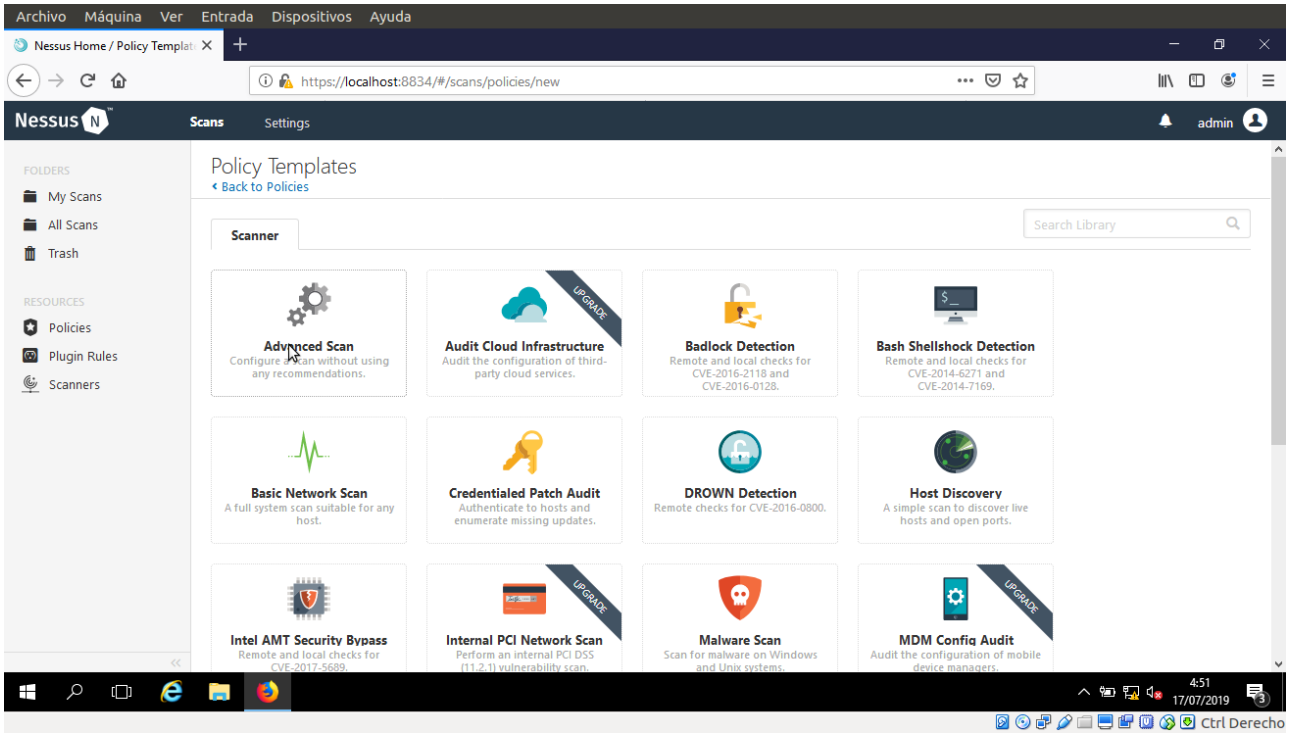


28. Para agregar una nueva política, haga clic en el botón Políticas en la barra de menú.

29. Se abre la ventana nessus / Policies, haga clic en el botón + Políticas nuevas.

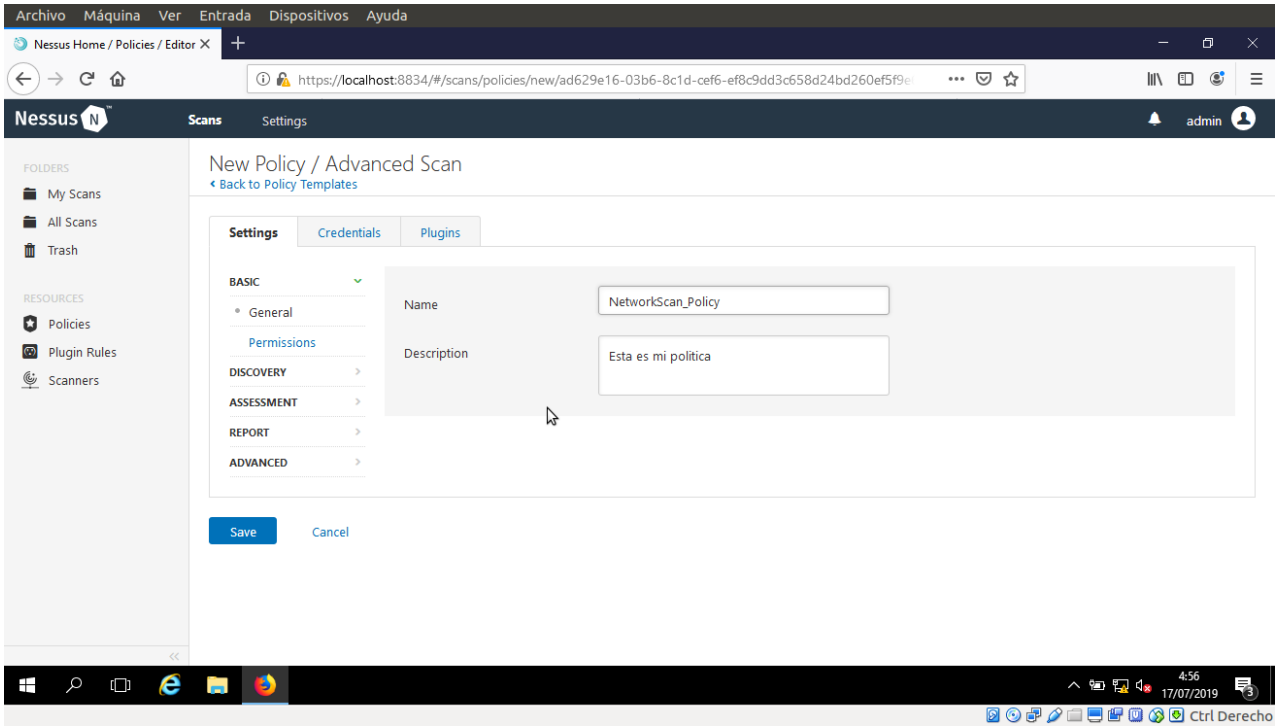


30. Aparece la ventana de asistentes de políticas, desplácese hacia abajo y haga clic en Política avanzada.



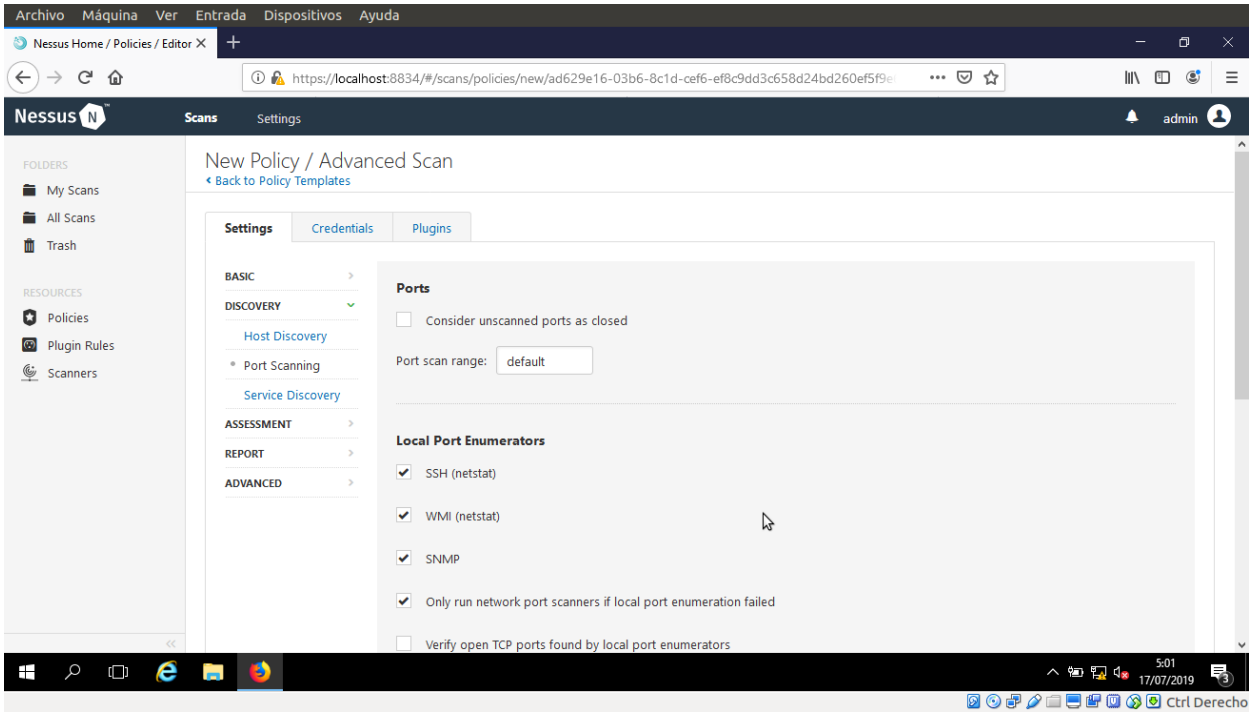
31. La sección de configuración general de la política con el tipo de configuración básica aparece.

32. Especifique un nombre de política en el campo de nombre (NetworkScan_policy) y proporcione una descripción de la política.

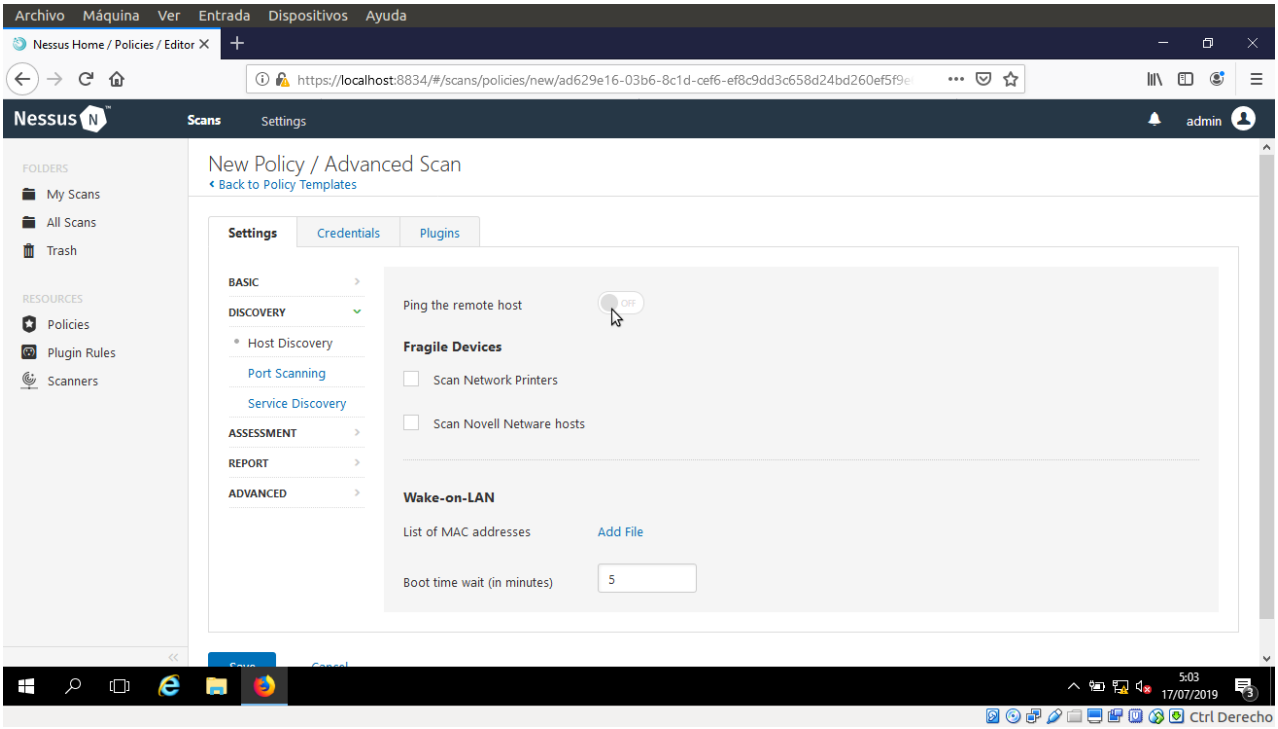


33. En el campo de tipo de configuración, seleccione escaneo de puertos de la lista desplegable.

34. Aparece la ventana de configuración general de la política con el tipo de configuración de escaneo del puerto, con las opciones predeterminadas, como se muestra en la siguiente captura de pantalla.

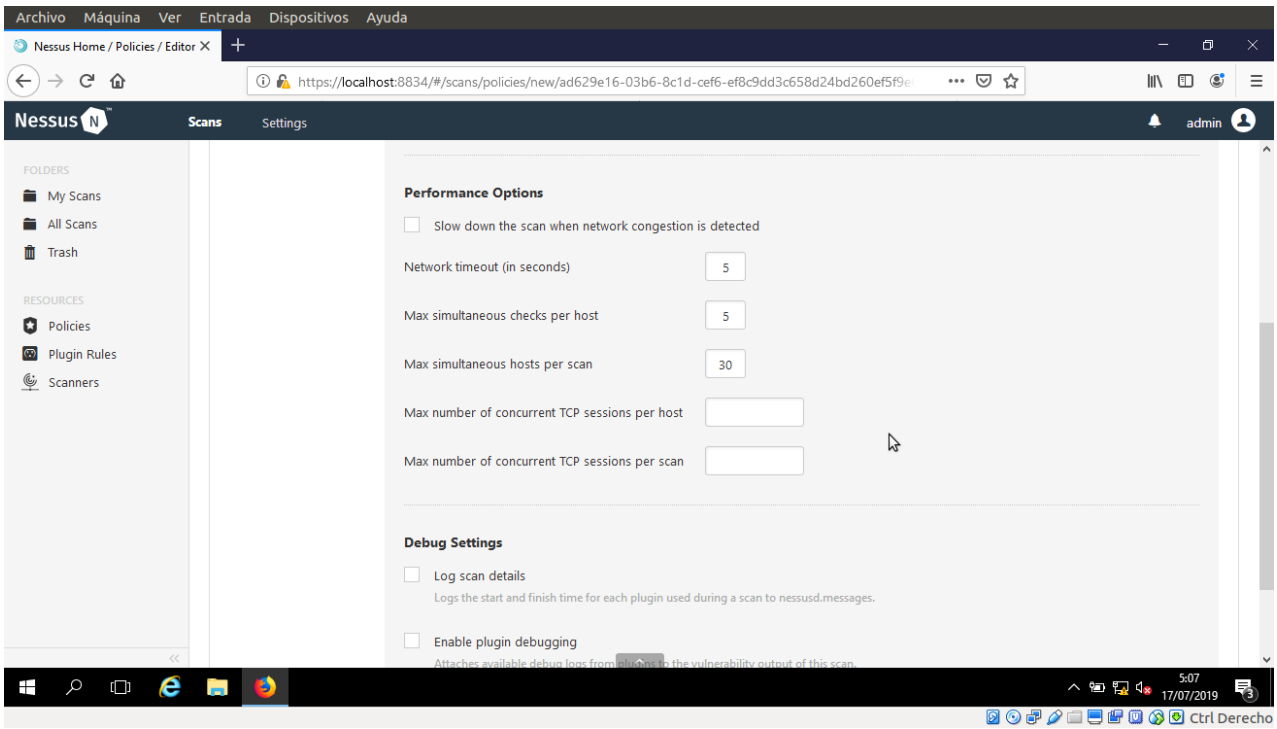


35. Desmarque la opción ping del host remoto y la opción del escáner TCP nessus.

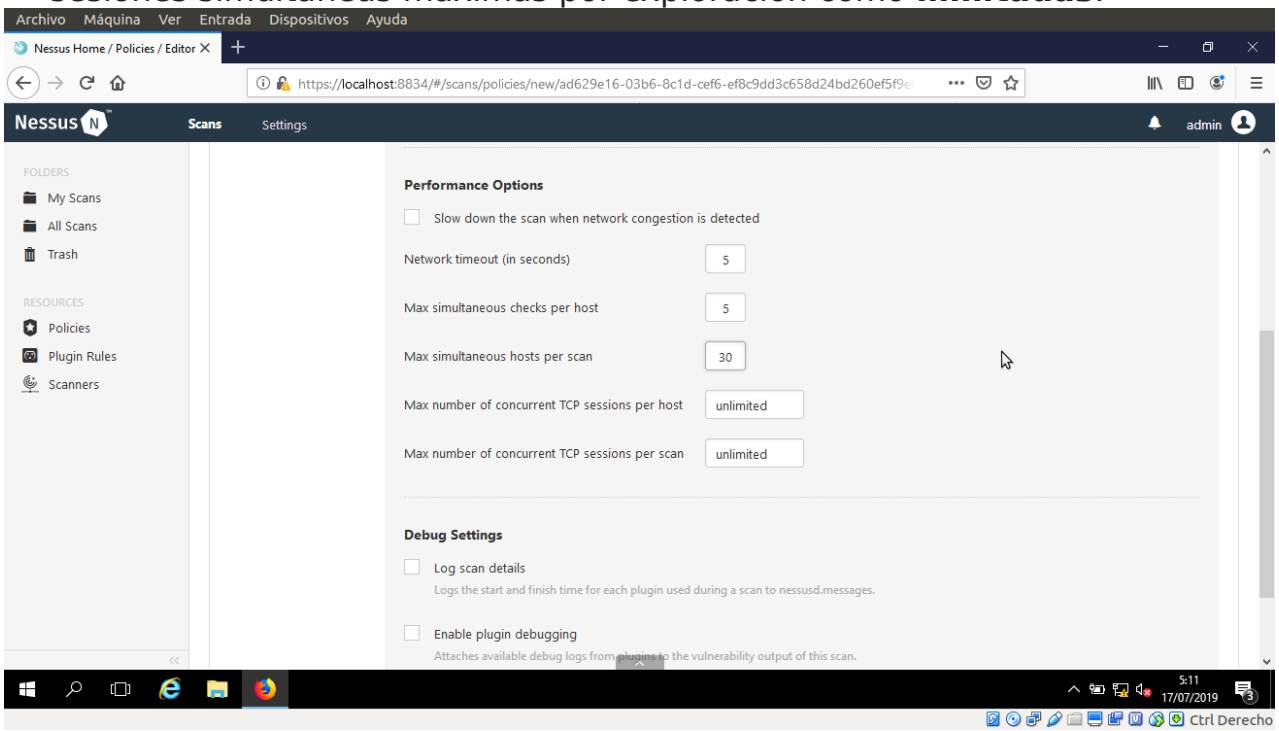


36. En el campo tipo de configuración, selecciona rendimiento de la lista deplegable.

37. En el campo tipo de configuración, aparece el tipo de configuración de rendimiento seleccionado, con las opciones predeterminadas como se muestra a continuación en la siguiente captura de pantalla.



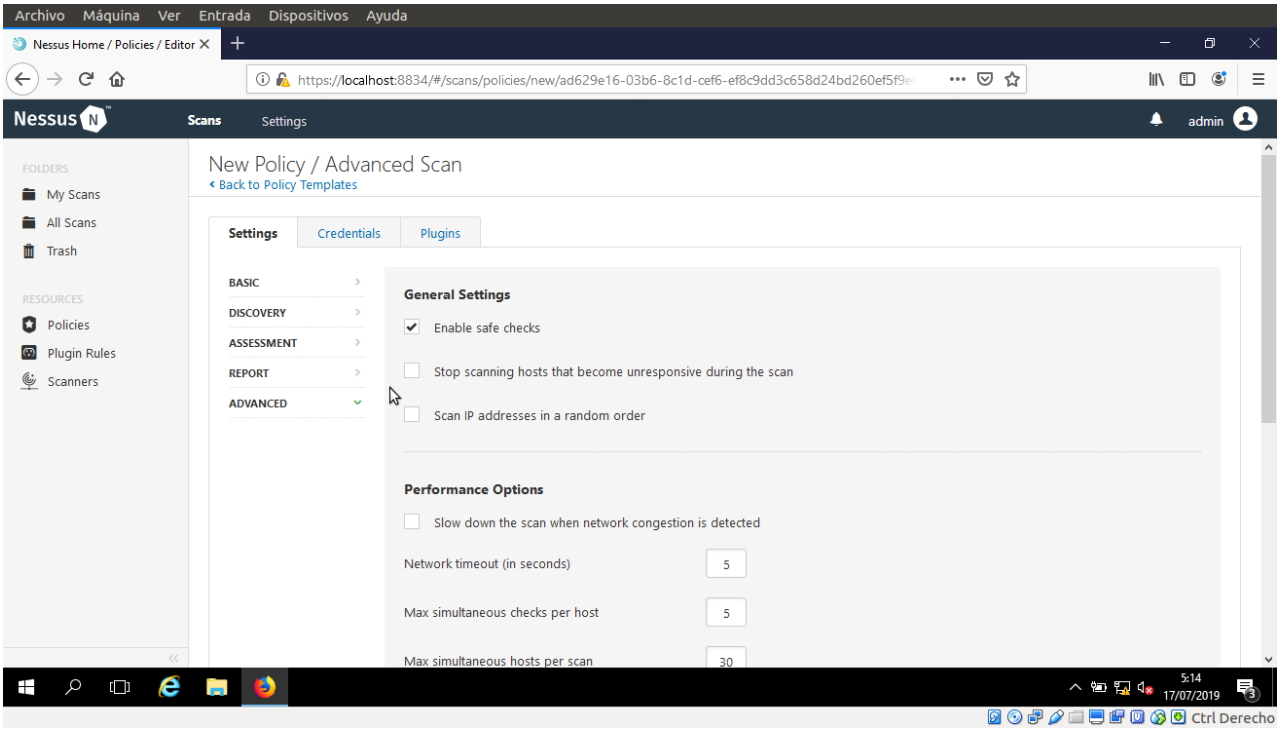
38. Establezca valores de sesiones TCP simultáneas máximas por host y sesiones simultáneas máximas por exploración como **ilimitadas**.



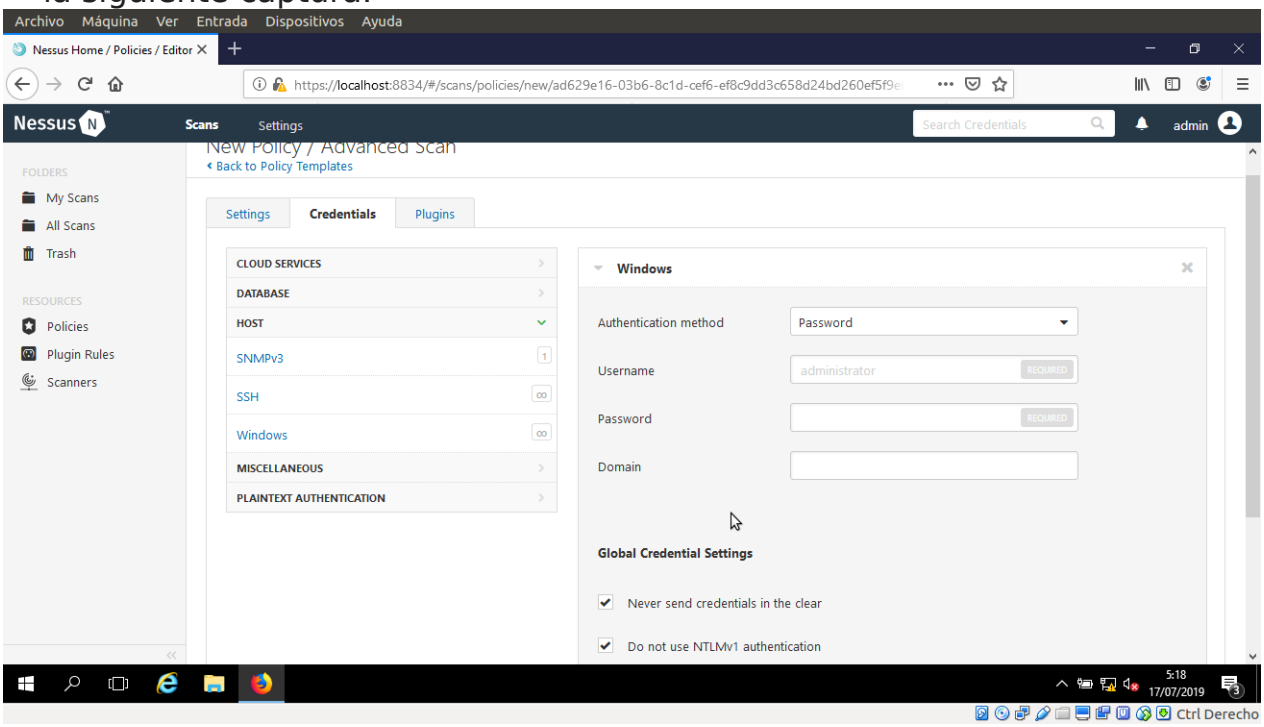
39. En el campo de tipo de configuracion, selecione **avanzado** de la lista desplegable.

40. Aparece la ventana de configuración general de la política con el tipo de configuracion avanzada.

41. No cambies la configuracion por defecto del campo de configuración.



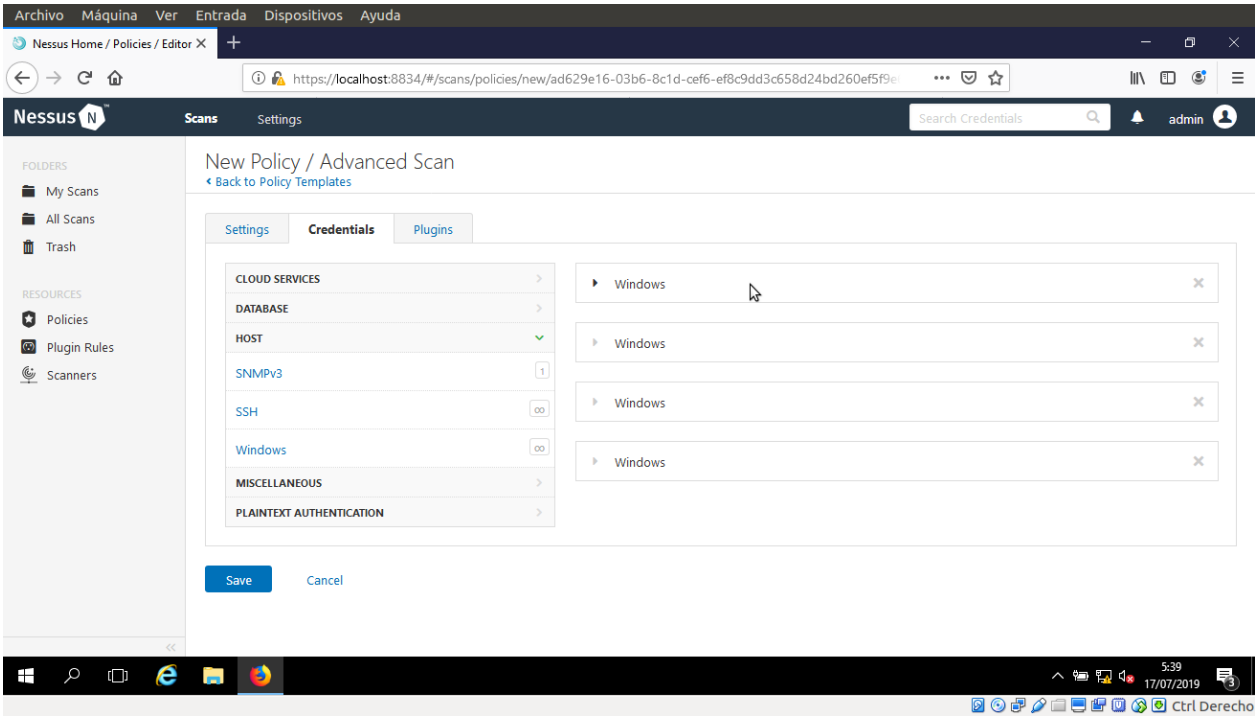
42. Para configurar las credenciales de una nueva politica, has click en Credenciales del panel izquierdo. Una nueva ventana con las politicas de credenciales, con credenciales de windows se mostrará, como se muestra en la siguiente captura.



43. Especifique los nombres de las cuentas SMB (**SMB account names**) (como se muestran en la captura de pantalla) y las contraseñas en la ventana. En Tipo de contraseña SMB (**SMB password type**), seleccione la opción de hashes NTLM (**NTLM hashes**) en la lista desplegable de tipo de contraseña SMB.

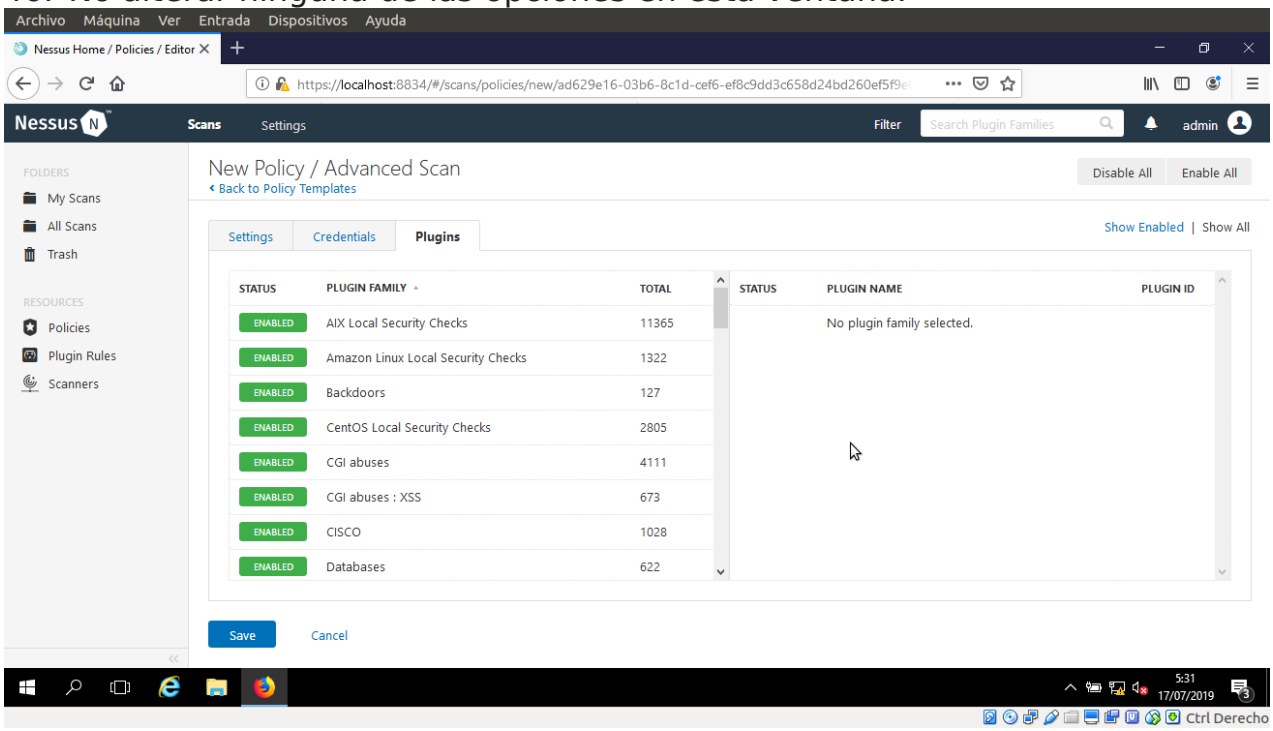
44. Aquí, especificará los dos nombres de cuentas SMB y sus respectivas contraseñas. Son los siguientes:

- **AD144, qwerty @ 123**
- **AD144, qwerty @ 123**
- **AD145, qwerty @ 123**
- **AD146, qwerty @ 123**



45. Para seleccionar los complementos requeridos, haga clic en la pestaña Complementos (**Plugins**) en el panel izquierdo.

46. No alterar ninguna de las opciones en esta ventana.



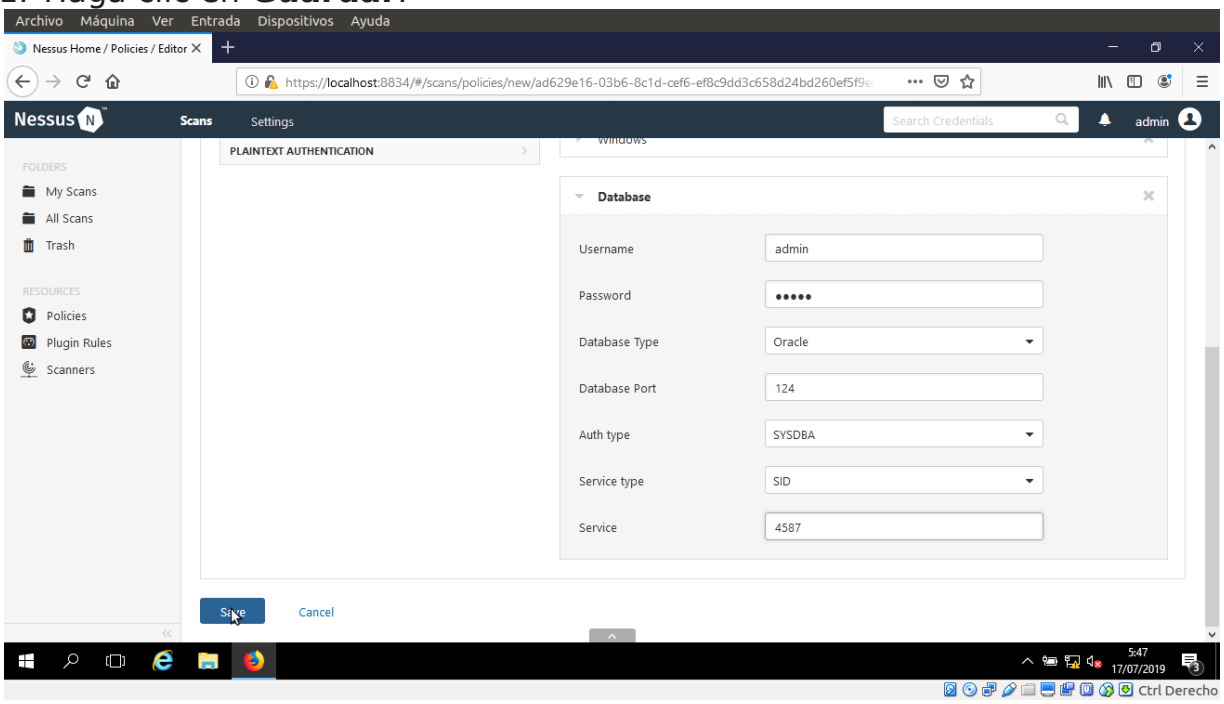
47. Para configurar las preferencias, haga clic en la pestaña Preferencias (**Preferences**) en el panel izquierdo.

48. En el campo Complemento (**Plugin**), seleccione Configuración de la base de datos (**Database settings**) en la lista desplegable.

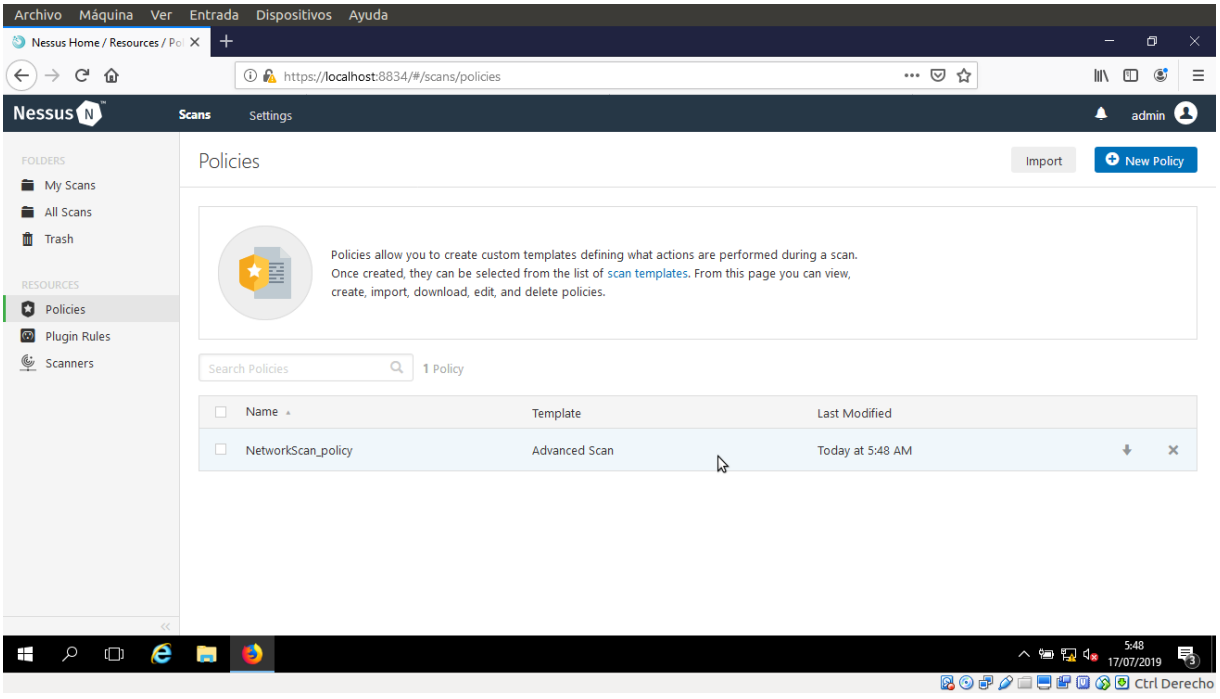
49. Ingrese los detalles de inicio de sesión (**Login**) ingresados al momento del registro.

50. Ingrese la base de datos SID: **4587**; Uso del puerto de la base de datos: **124**; y seleccione el tipo de autenticación Oralcle: **SYSDBA**.

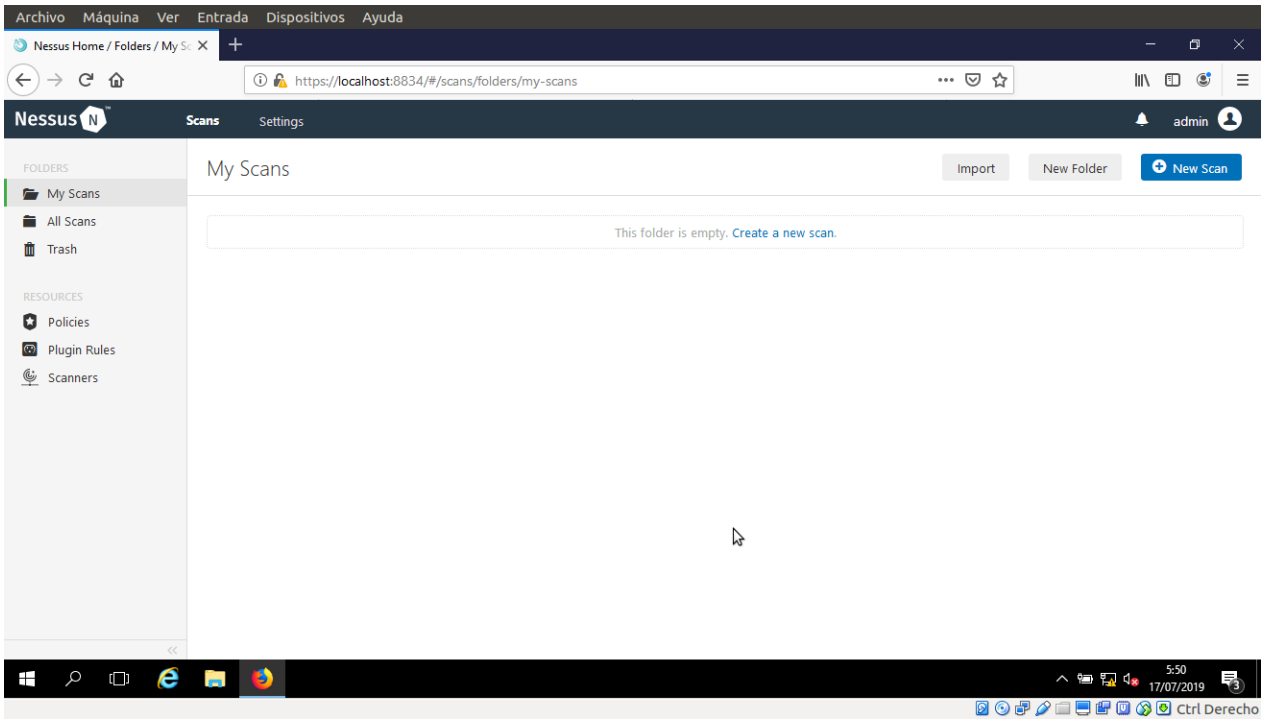
51. Haga clic en **Guardar**.



52. Una política se actualizó correctamente (**Policy updated successfully**), y la política se agrega como en la ventana Nessus / Policies, como se muestra en la siguiente captura de pantalla.

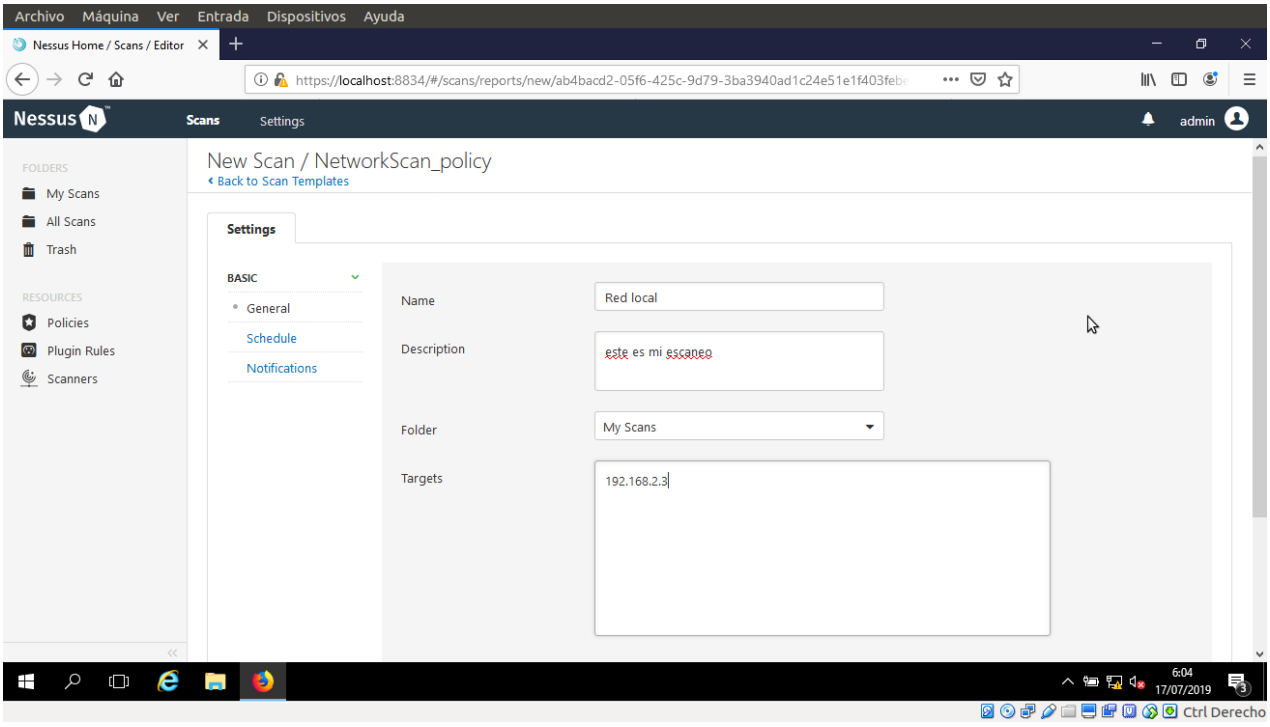


53. Ahora, haga clic en Exploraciones -> + Nueva exploración (**Scans -> +New Scan**) para abrir la Nueva plantilla de exploración (**New Scan Template**).

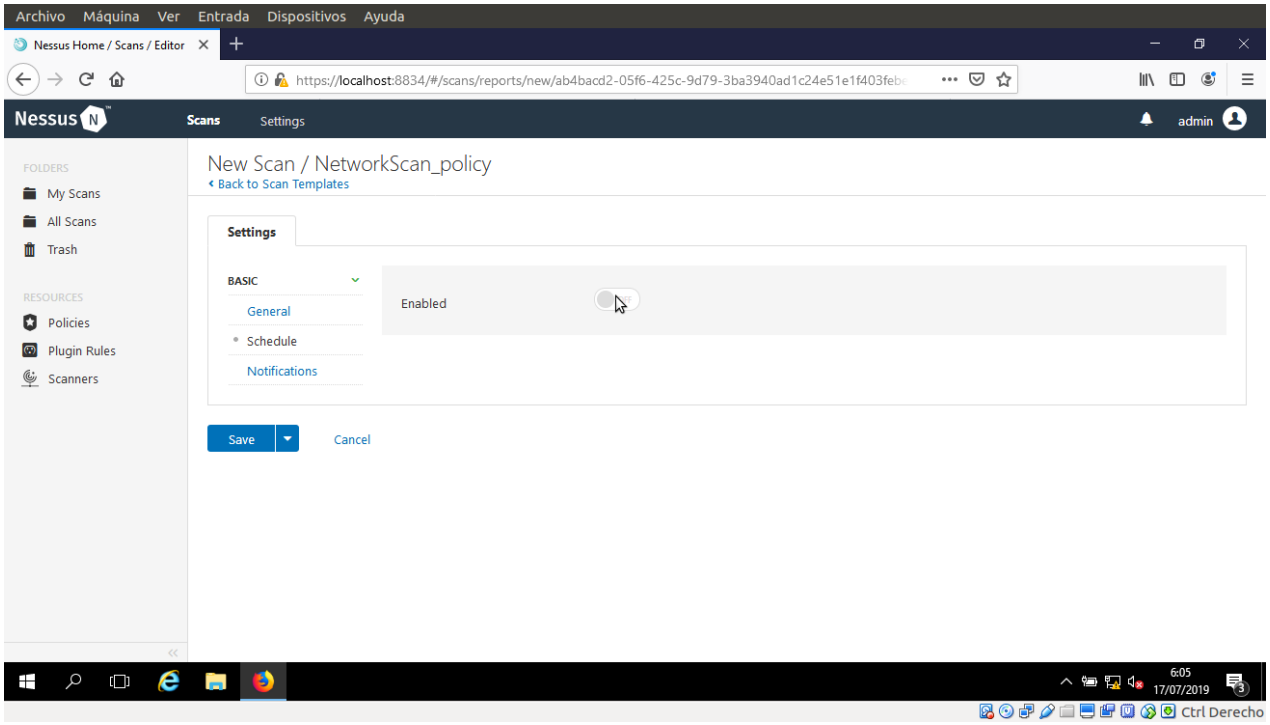


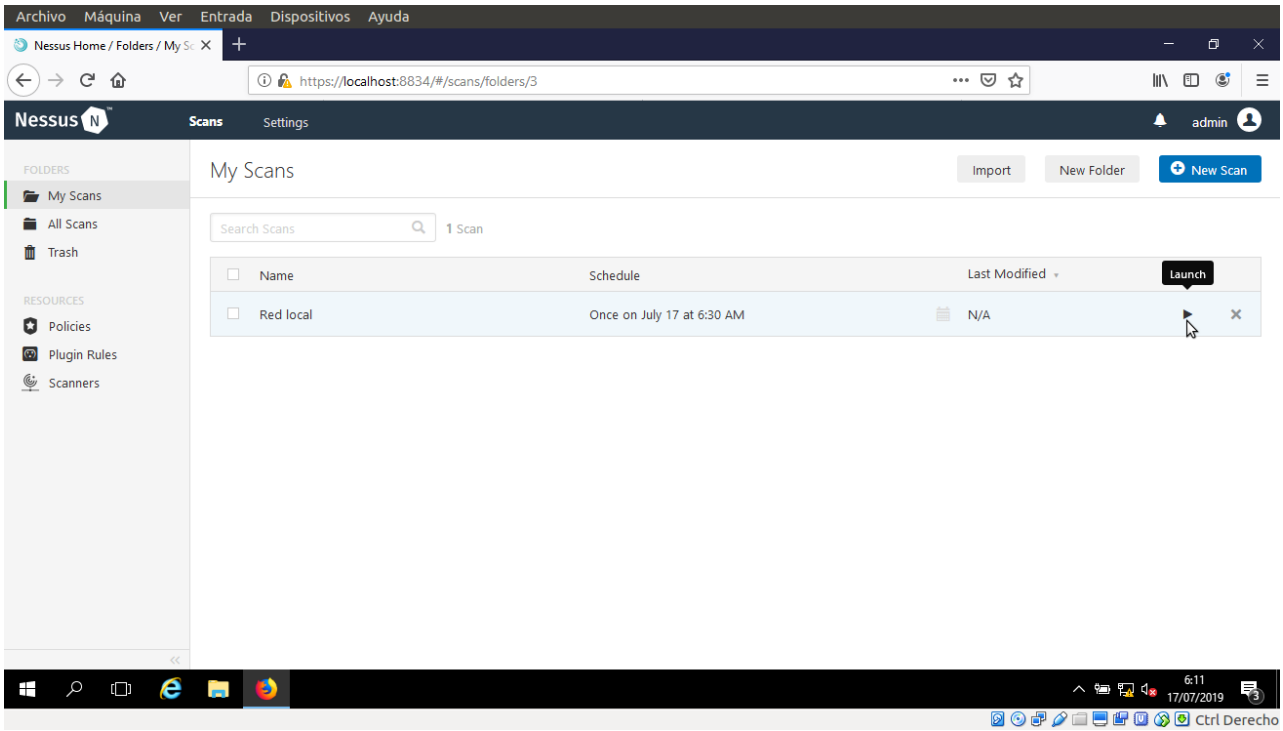
54. Ingrese el Nombre (**Name**) del escaneo (aquí, Red local), ingrese la Descripción (**Description**) para el escaneo y elija **NetworkScan_Policy** en la lista desplegable de Políticas (**Policy**).

55. En los destinos de escaneo (**Scan Targets**), ingrese la dirección IP del objetivo en el que desea realizar la evaluación de vulnerabilidad. En esta práctica de laboratorio, es una máquina virtual de **Windows** cuya dirección IP es <**192.168.2.3**>.

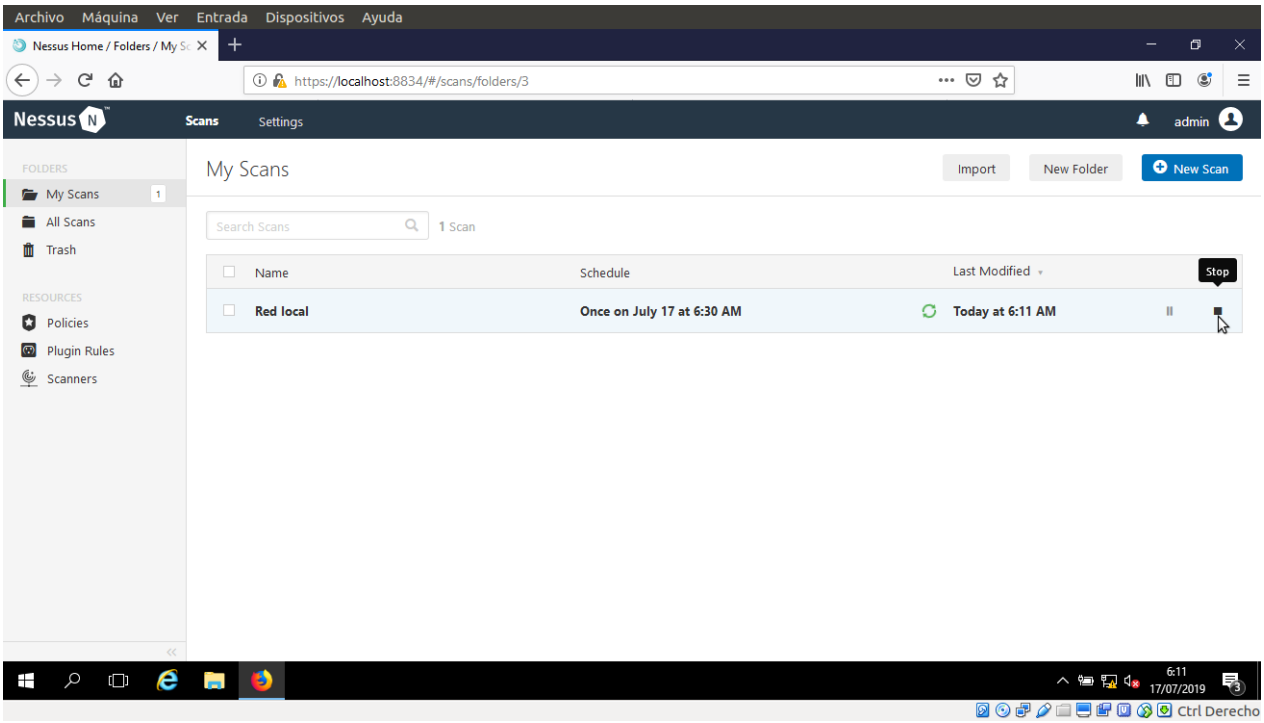


56. Haga clic en Configuración de la programación (Schedule Settings) en el panel izquierdo, seleccione Ahora en la lista desplegable Iniciar (**Launch**) y haga clic en Iniciar (**Launch**).



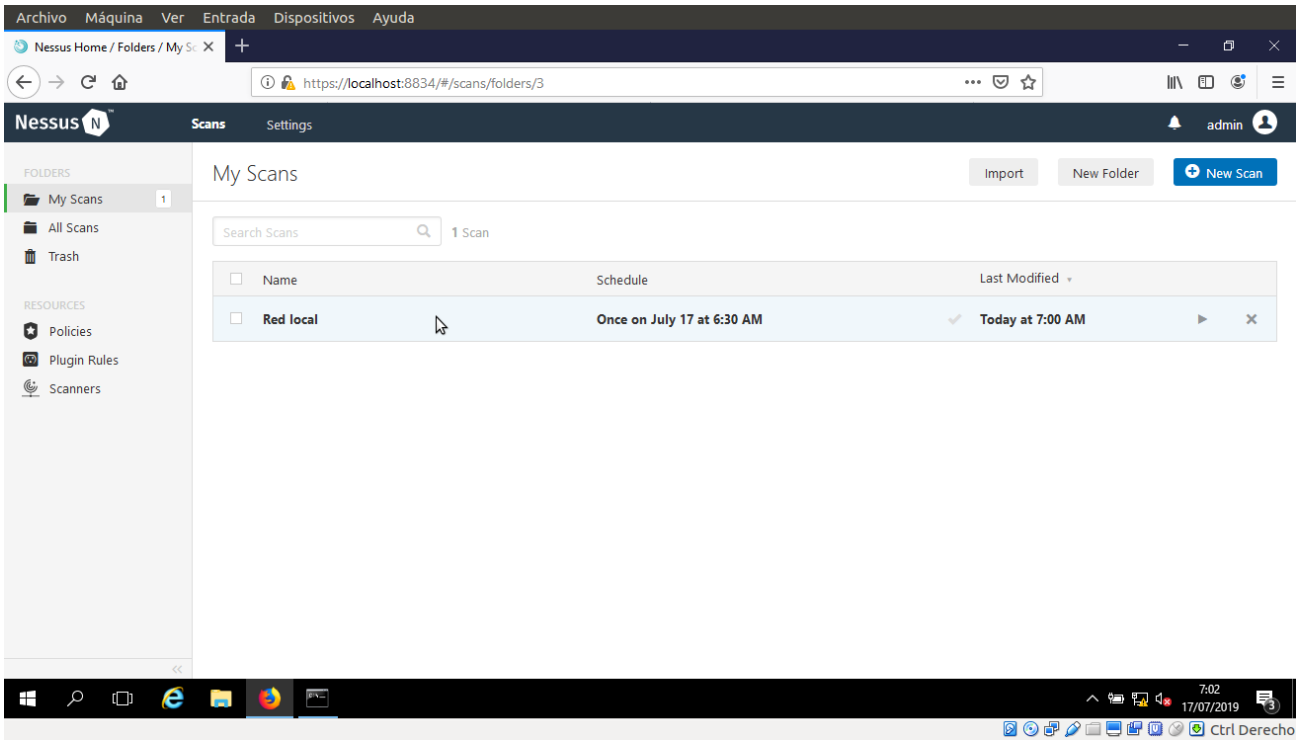


57. Se inicia el escaneo y Nessus comienza a escanear el objetivo.

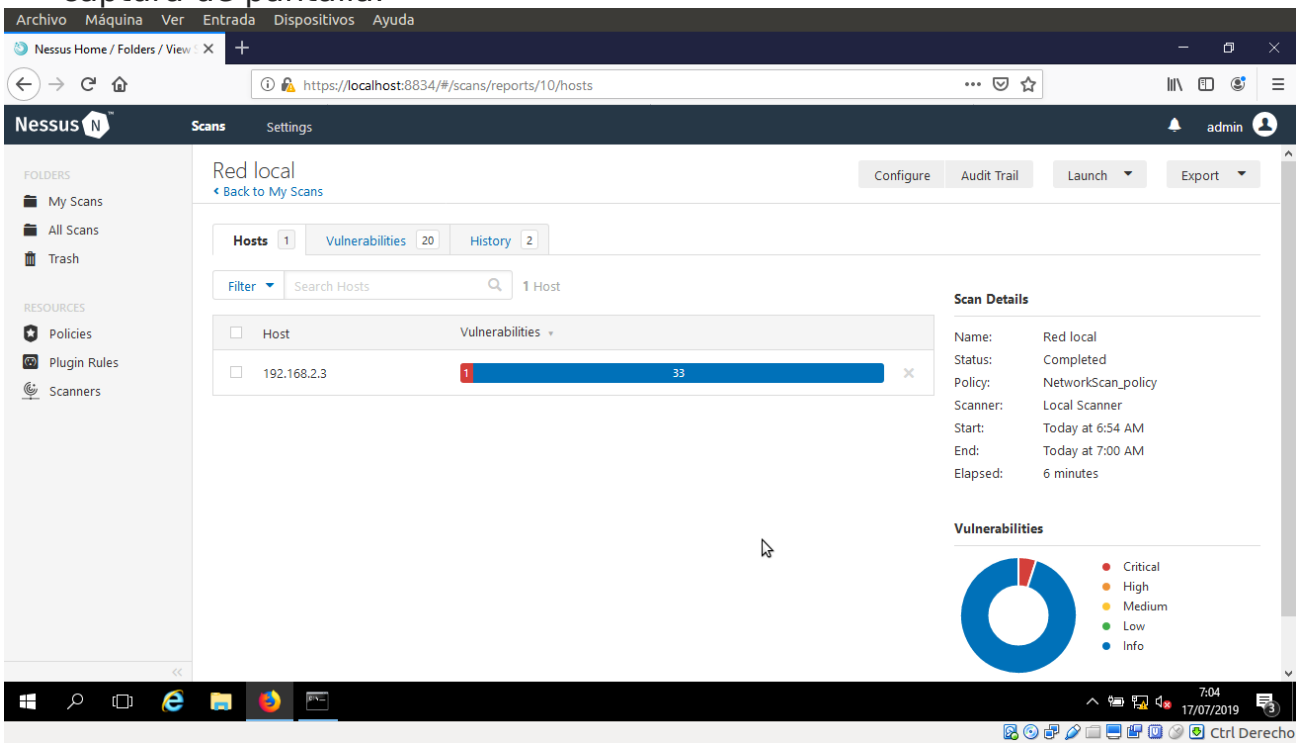


58. Una vez finalizada la exploración, el estado de la exploración cambia a Completado (**Completed**).

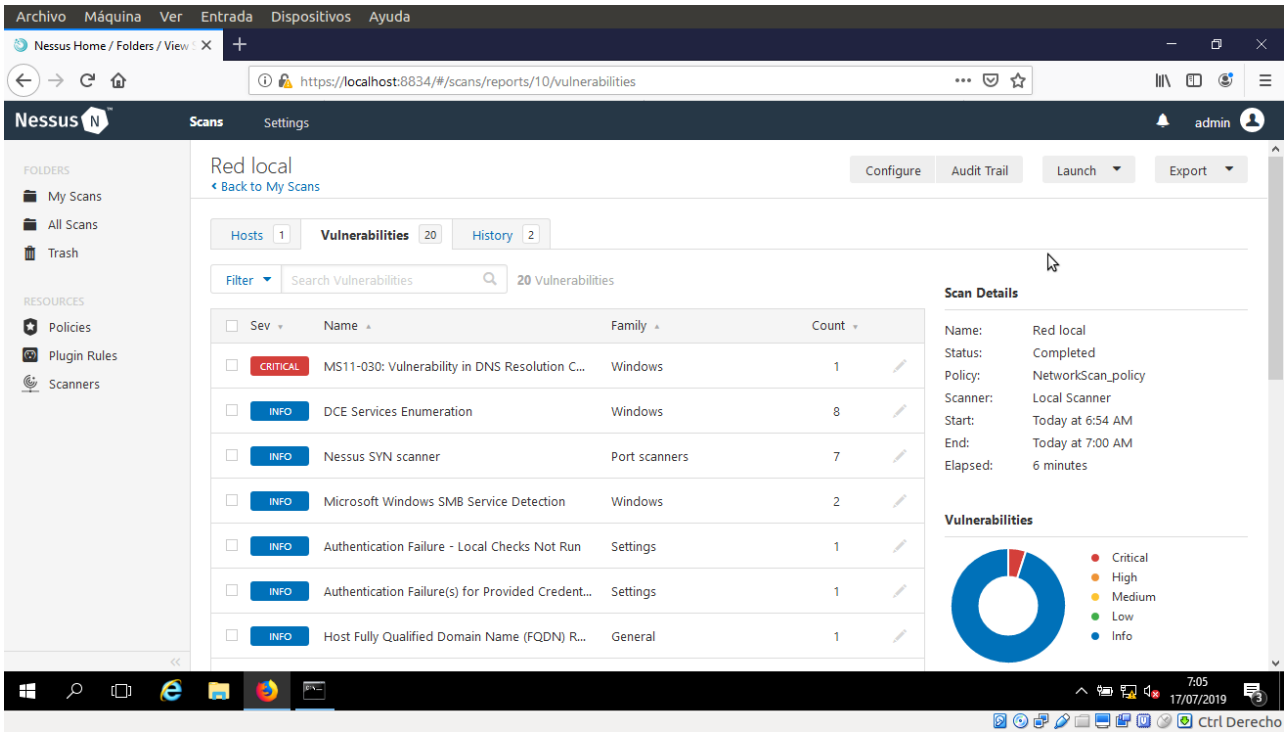
59. Haga clic sobre el para ver los resultados detallados.

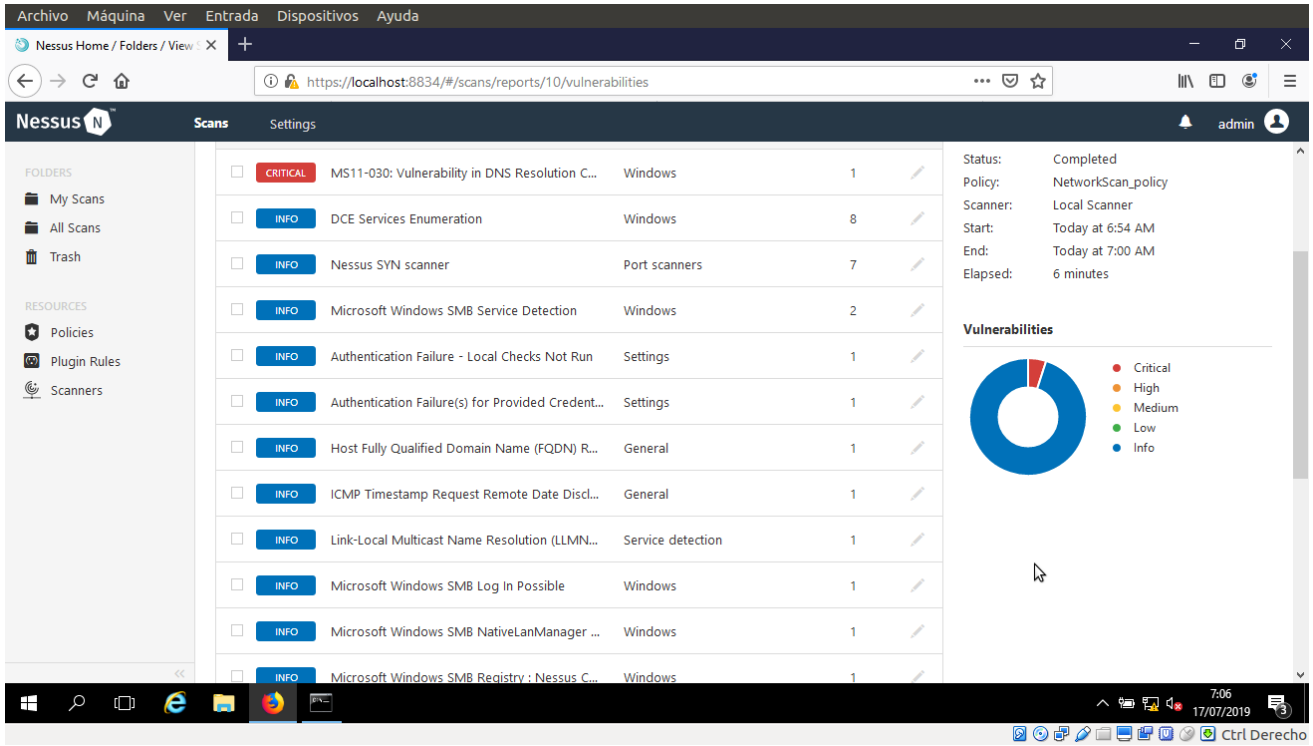


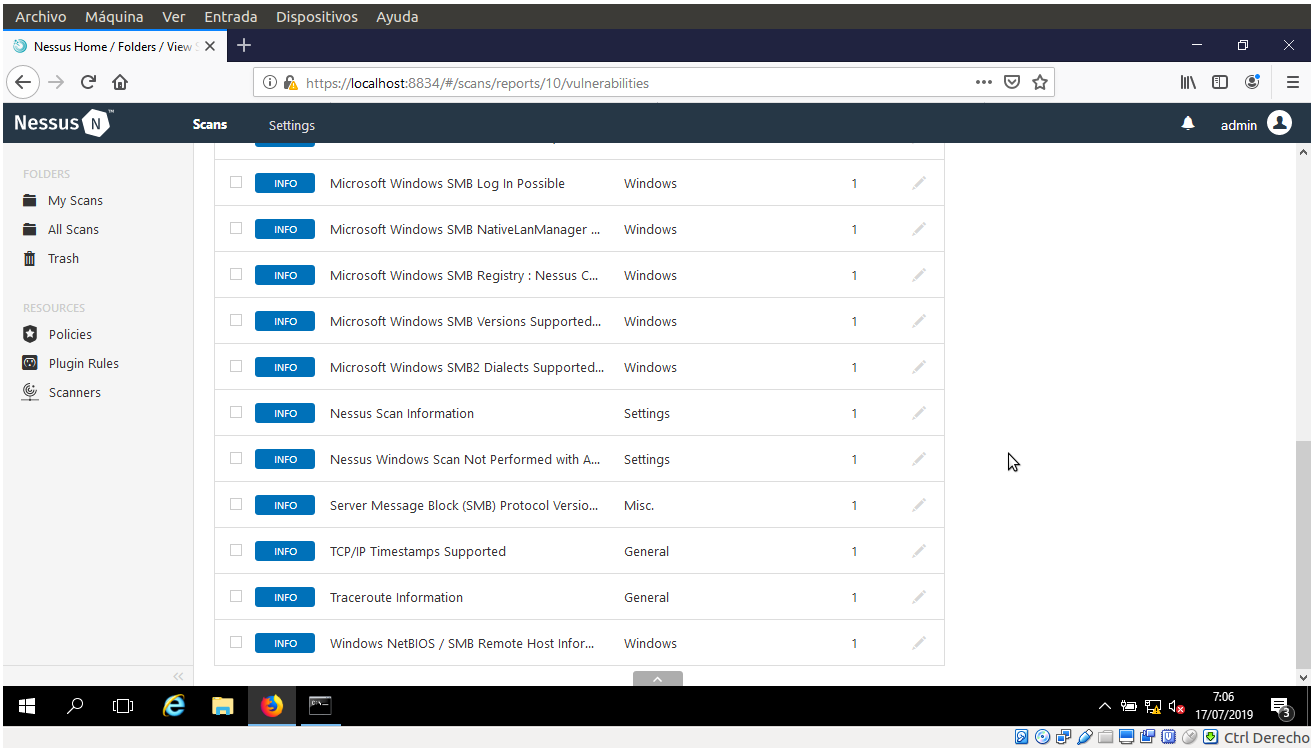
60. Se abre la ventana de la red local, que muestra el resumen de los hosts y los detalles del escaneo (**Scan Details**), como se muestra en la siguiente captura de pantalla.



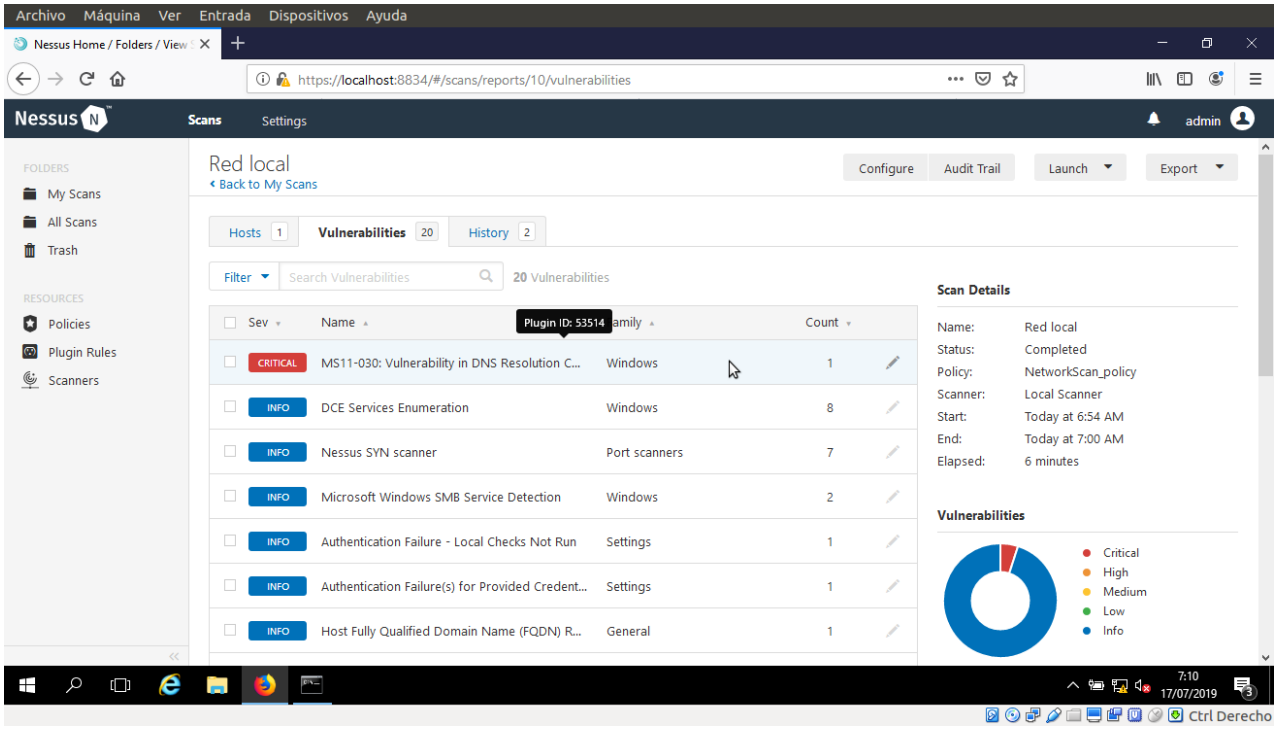
61. Haga clic en la pestaña de vulnerabilidades y desplácese hacia abajo en la ventana para ver todas las vulnerabilidades asociadas con la máquina de destino.



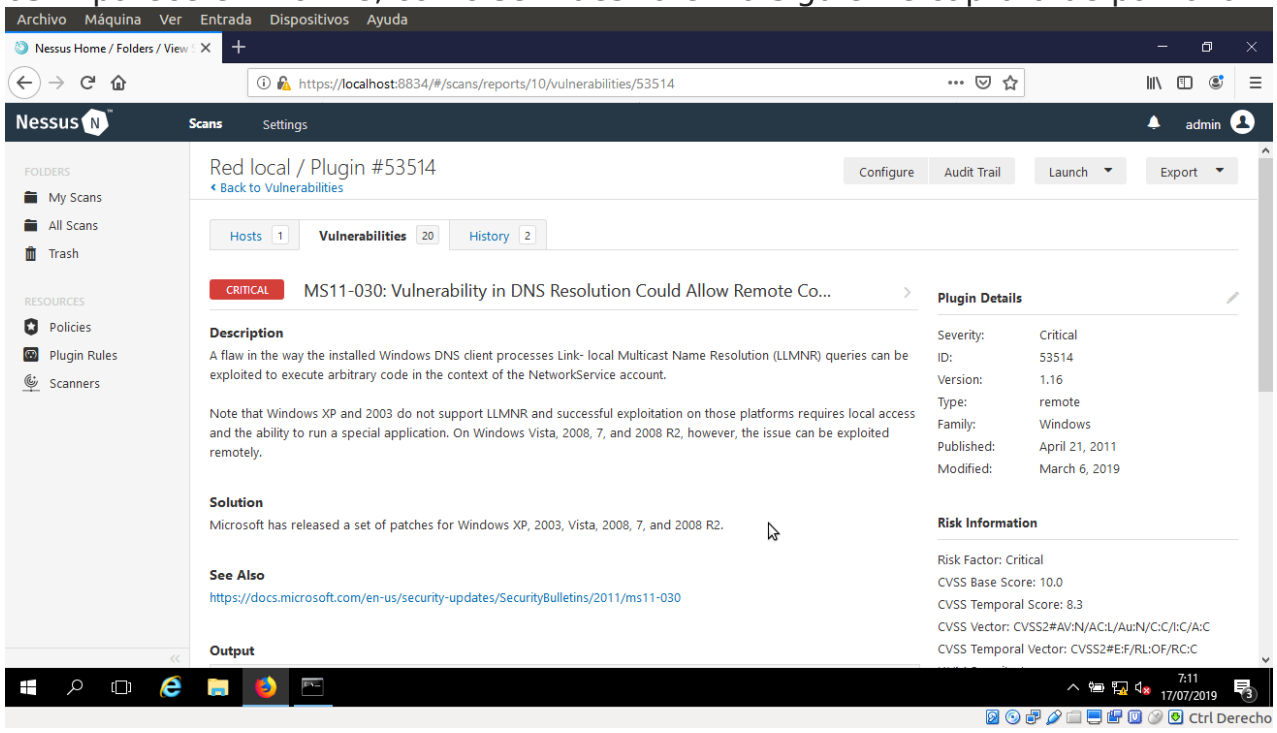




62. Haga clic en estas vulnerabilidades para ver un informe detallado sobre cada una de ellas. Para instante, en este laboratorio, MS11-030; Se ha seleccionado la vulnerabilidad **DNS Resolution Could Allow Remote Code Execution** de Microsoft Windows.

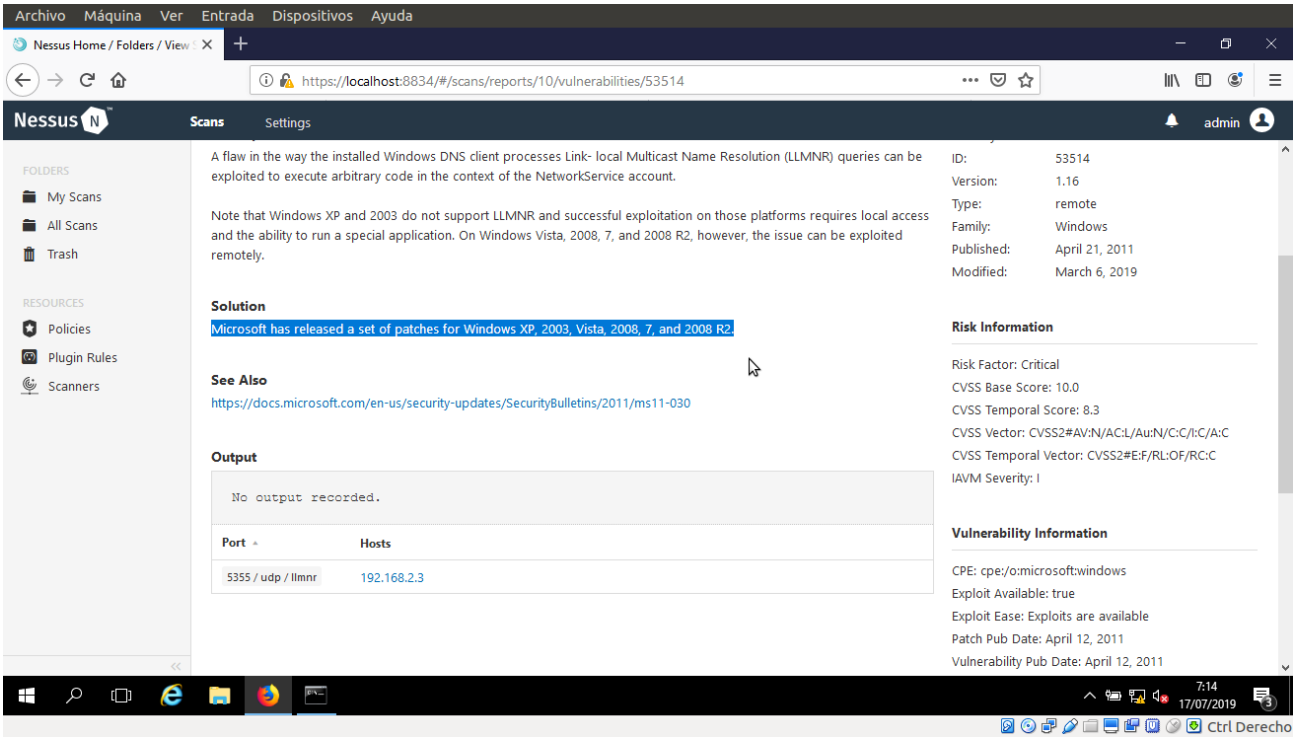


63. Aparece el informe, como se muestra en la siguiente captura de pantalla.



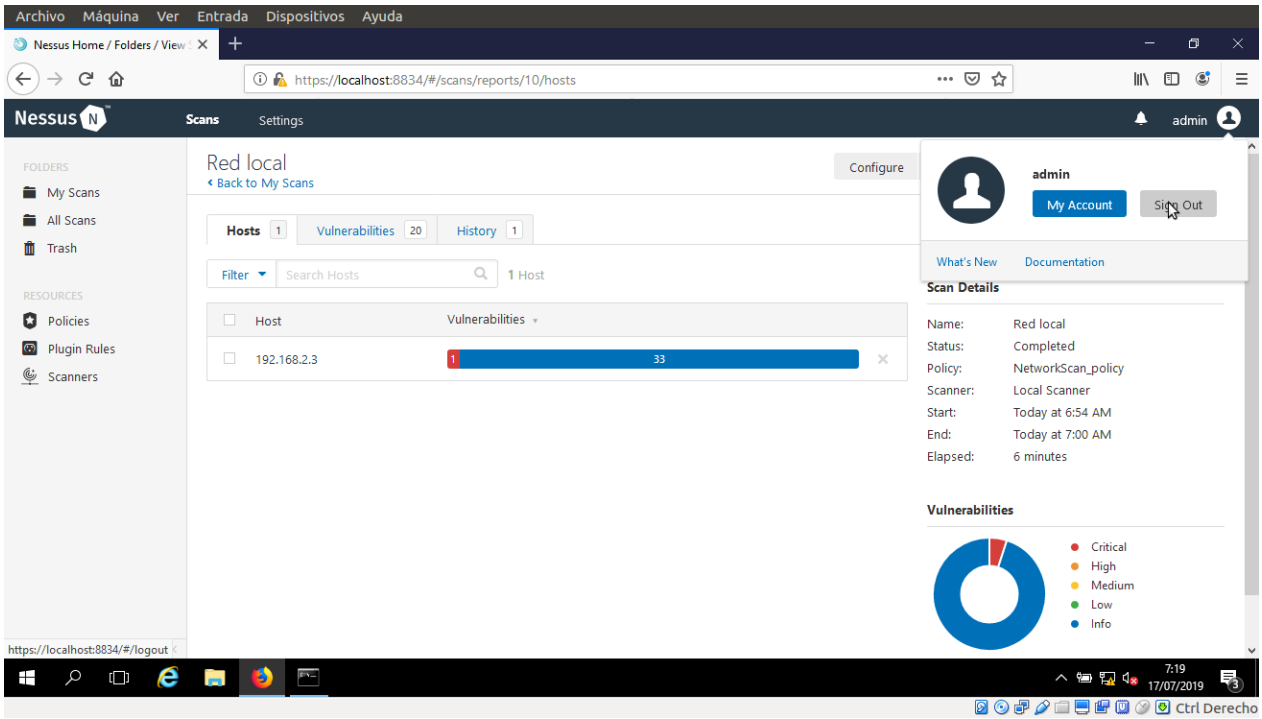
64. En tiempo real, un atacante examina las vulnerabilidades relacionadas con el objetivo y desarrolla un exploit adecuado para resolverlo. Haga clic en la pestaña Remediaciones para ver las recomendaciones que lo ayudarán a resolver ciertas vulnerabilidades en la red.

Nota: En la version mas actual de Nessus las recomendaciones son especificadas en cada error en la pestaña vulnerabilidades.

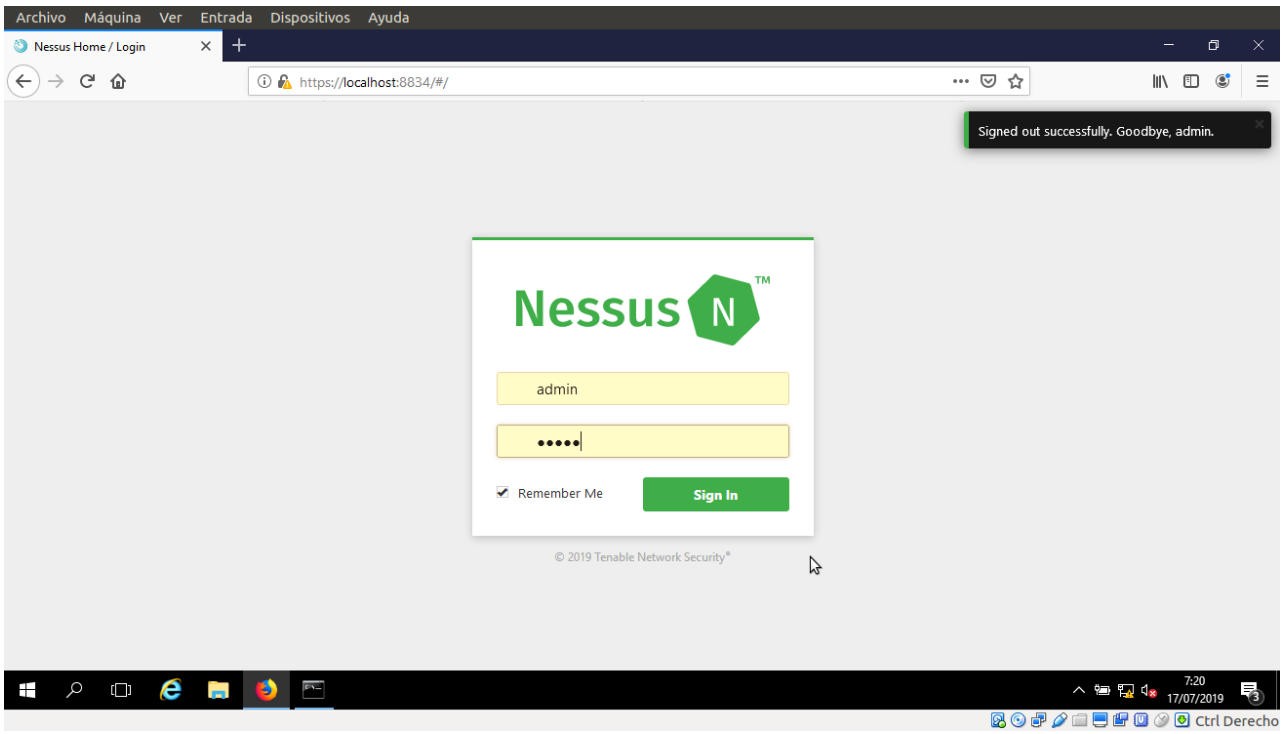


65. Haga clic en la pestaña Notas para ver las notas de escaneo.

66. Al completar el análisis de vulnerabilidad, haga clic en admin -> Cerrar sesión.

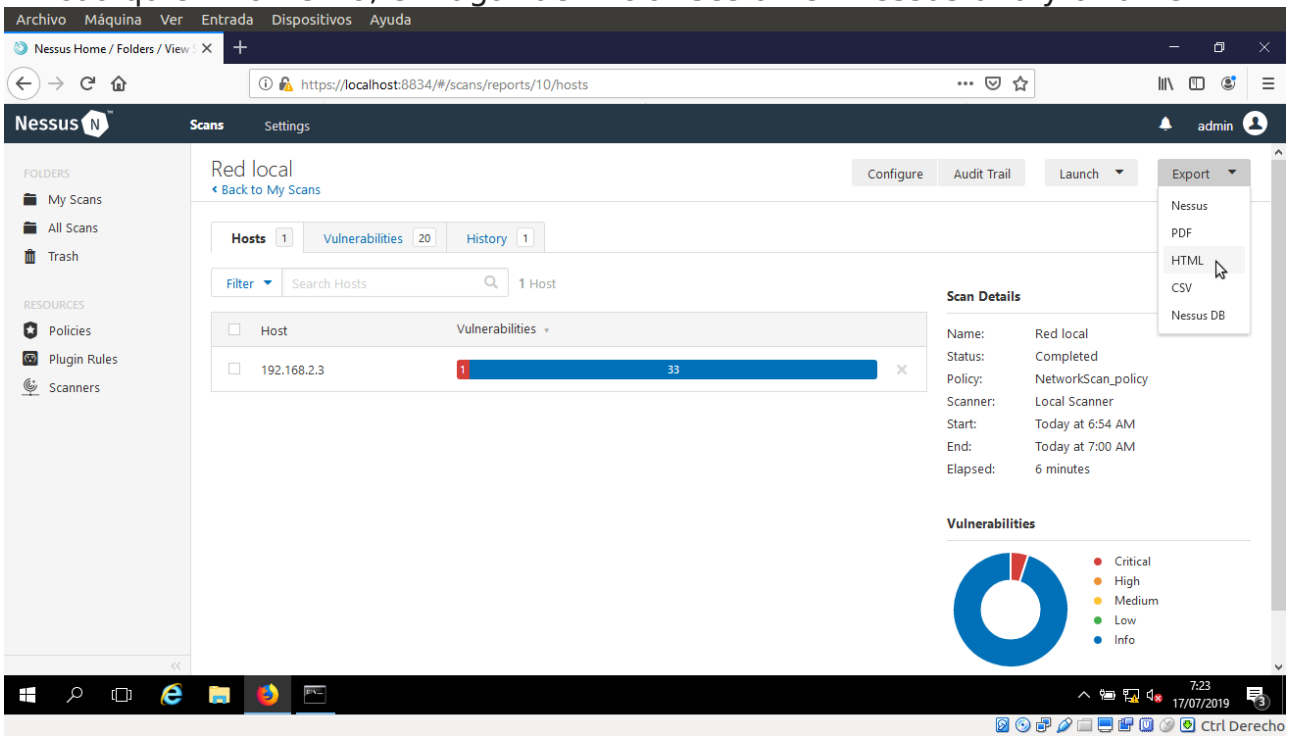


67. Una vez que la sesión finaliza con éxito, aparece la siguiente ventana, con el estado de bloqueo: **la sesión del usuario se destruyó con éxito. Adiós admin** Cierra el navegador.



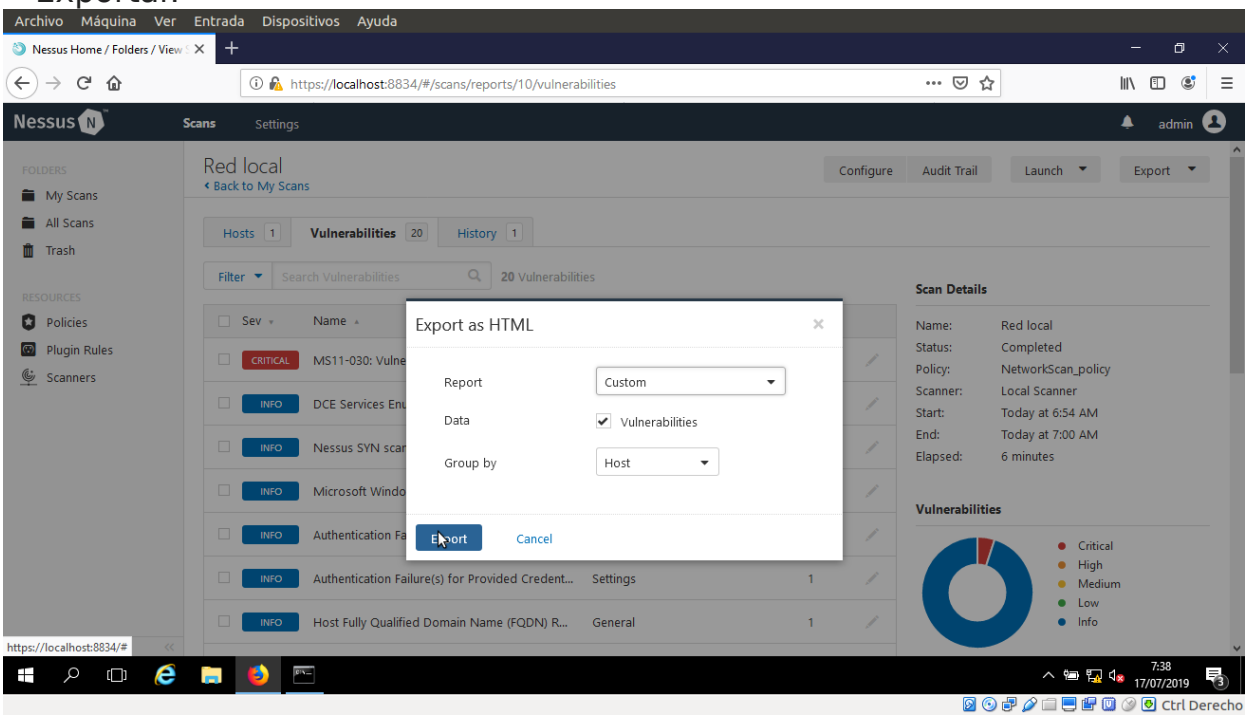
68. Para descargar un informe, inicie sesión en Nessus, abra la sección de escaneos y seleccione el escaneo de la red local.

69. Haga clic en la pestaña Exportar y elija un formato de archivo (aquí, HTML) de la lista desplegable. Al descargar un informe, puede acceder a él en cualquier momento, en lugar de iniciar sesión en nessus una y otra vez.

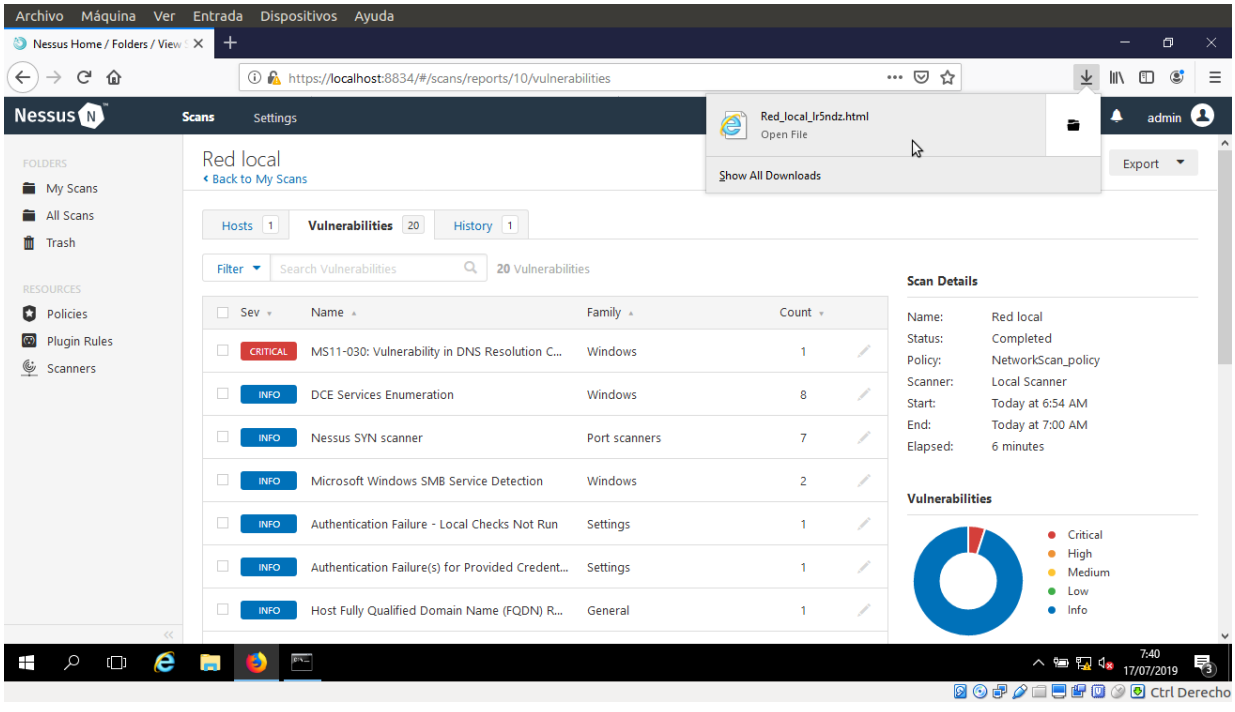


70. Se abre la ventana **Selección de capítulo HTML**, con dos secciones: Contenido disponible y Contenido del informe. La sección Contenido disponible contiene todos los informes (capítulos) que están disponibles relacionados con el análisis. Debe elegir los capítulos que desea descargar y arrastrarlos a la sección Contenido del informe. Los capítulos que se agregan a la sección Contenido del informe se descargarán.

71. En este laboratorio, todos los capítulos han sido seleccionados. Después de arrastrar el contenido que elige descargar como informe, haga clic en Exportar.



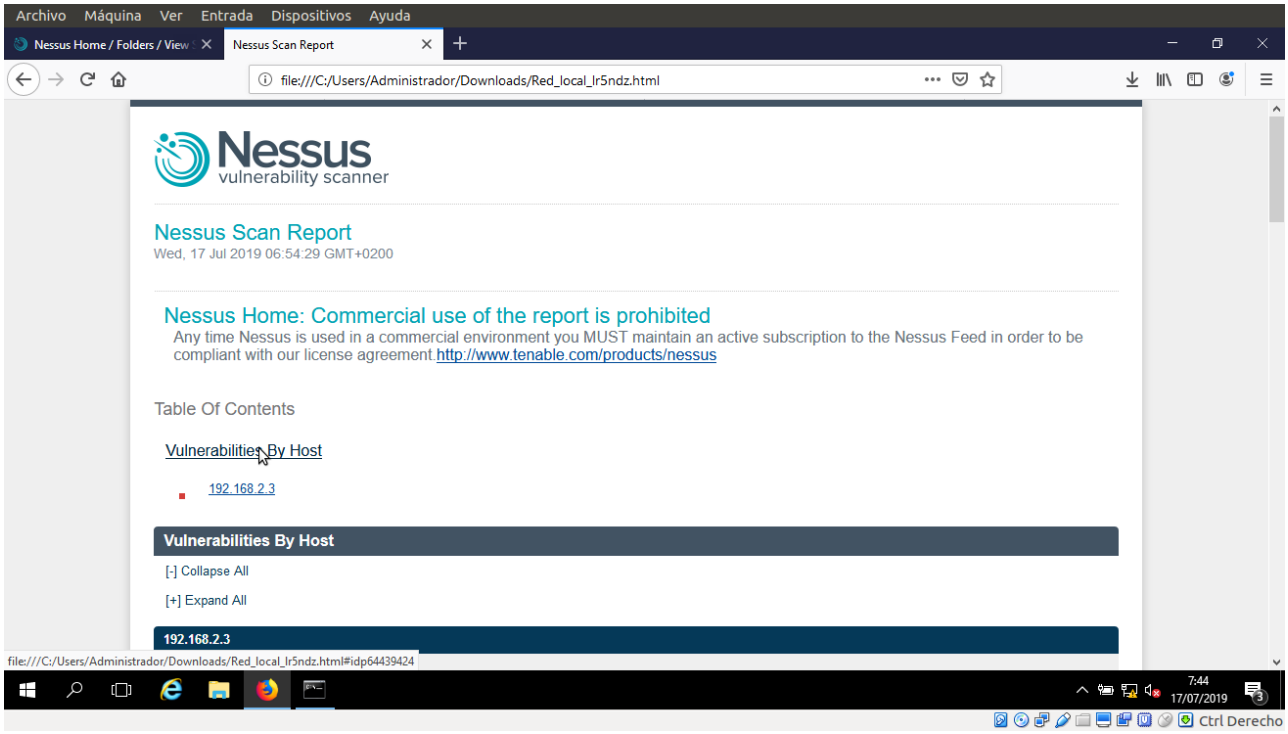
72. El archivo comienza a descargarse. Al finalizar la descarga, navegue hasta la ubicación donde se descargó el archivo y ábralo.



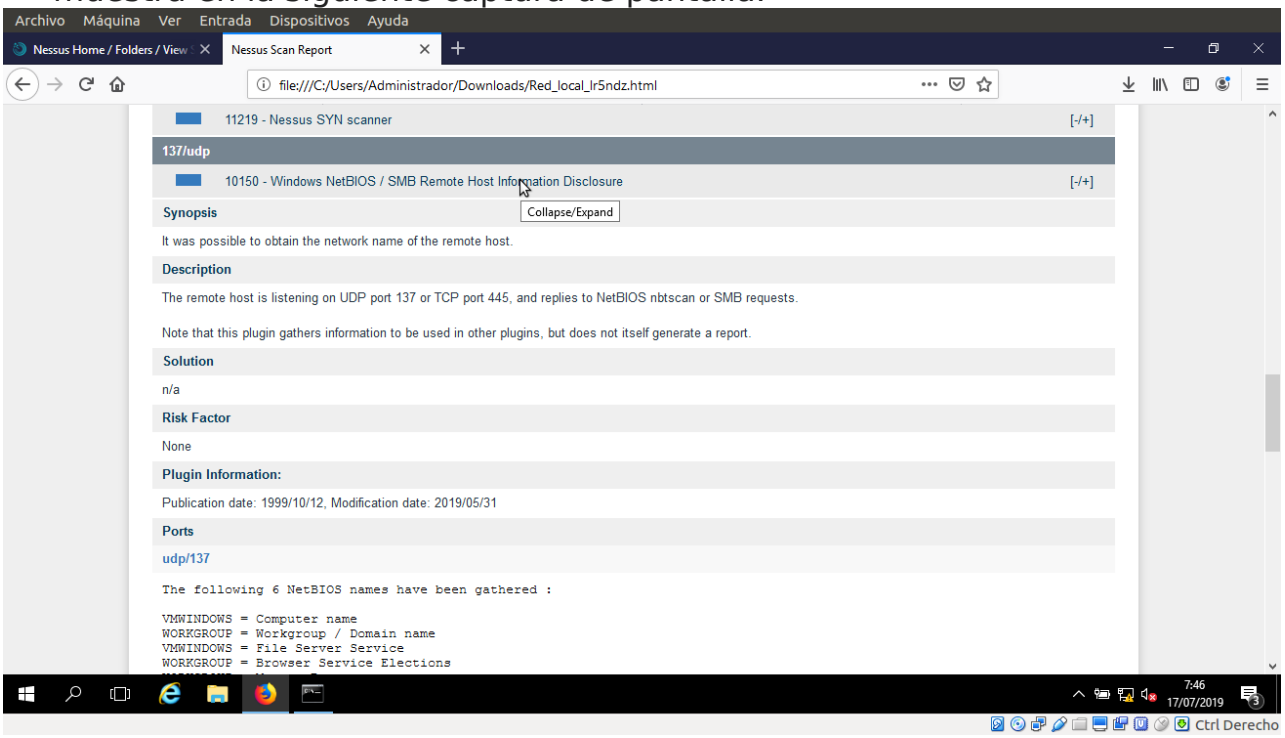
73. Elija un navegador para ver el archivo HTML.

74. El informe de exploración de Nessus aparece en el navegador web, como se muestra en la siguiente captura de pantalla.

75. Puedes elegir un capítulo de la lista de la tabla de centenos haciendo clic en él.

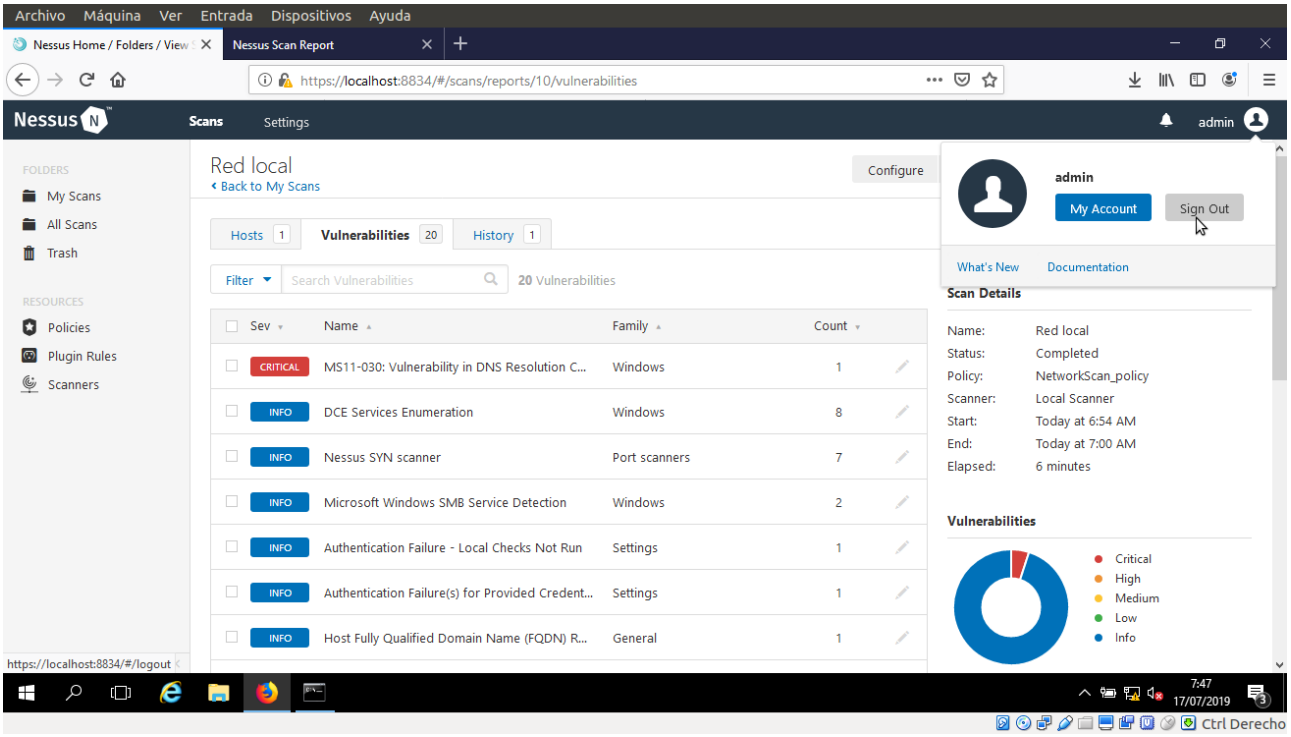


76. Los detalles de la vulnerabilidad seleccionada se enumeran como se muestra en la siguiente captura de pantalla.



77. De esta manera, puede seleccionar una vulnerabilidad de su elección para ver los detalles completos de la vulnerabilidad.

78. Una vez que esté realizando el análisis de vulnerabilidad, haga clic en -> **Salir**.



79. Una vez que la sesión se cierra correctamente, aparece la siguiente ventana, que dice: **La sesión del usuario se destruyó exitosamente. Adios admin.** Cierra el navegador.