Enumerar los recursos de red utilizando Advanced IP Scanner

Advanced IP Scanner es un escáner de red gratuito que proporciona diversos tipos de información con respecto a las computadoras de la red local.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a realizar un escaneo de la red local y descubrir todos los recursos de la red:

Necesitas :

- Realizar un escaneo del sistema y de la red.
- Enumerar cuentas de usuario
- Ejecutar penetración remota
- Recopilar información sobre la red local.

Visión general de la Network Scanning

La exploración de la red se realiza para recopilar información sobre sistemas en vivo, puertos abiertos y vulnerabilidades de la red. La información recopilada es útil para determinar las amenazas y vulnerabilidades de la red, y para saber si existen conexiones IP sospechosas o no autorizadas que podrían permitir el robo de datos y causar daños a los recursos.

Tareas del laboratorio

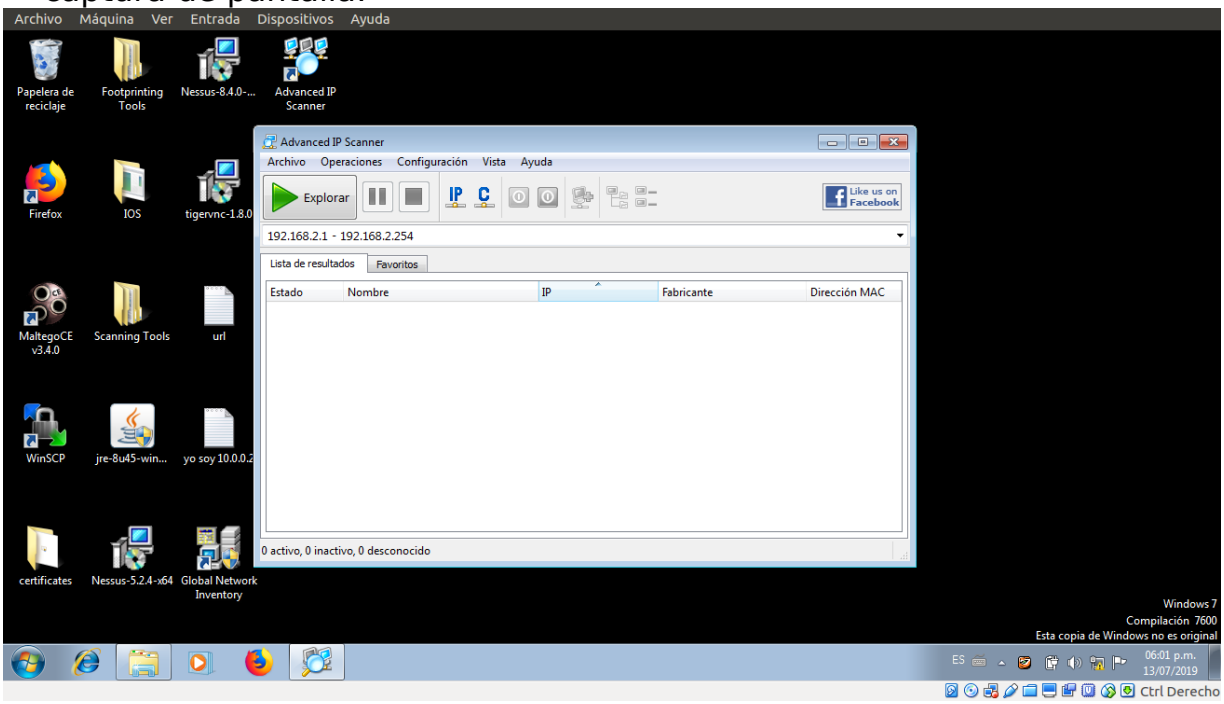
1. Navega hasta el directorio donde tengas almacenado el ejecutable del programa presiona **doble click**.

2. Si aparece la ventana emergente de archivo abierto, haga clic en Ejecutar.

3. Siga los pasos del asistente para instalar la de Advanced IP Scanner.

4. Al completar la instalación, inicie Advanced IP Scanner desde la pantalla de aplicaciones.

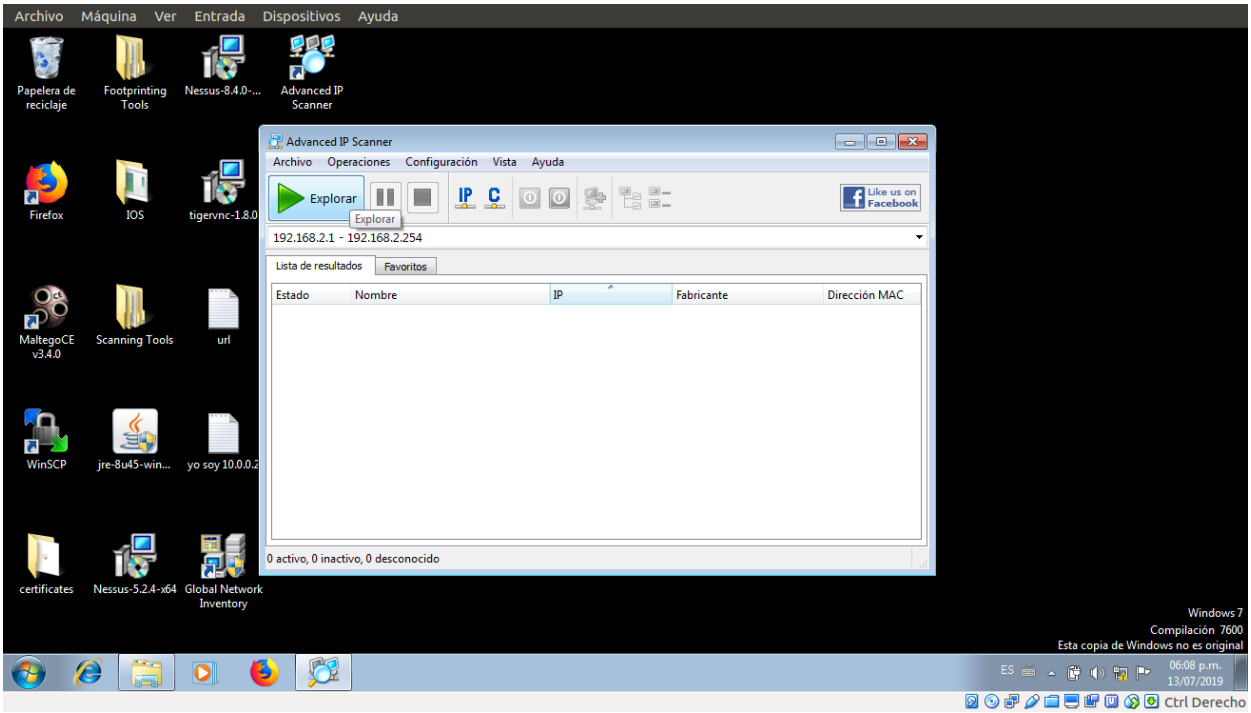
5. Aparece la GUI de Advanced IP Scanner, como se muestra en la siguiente captura de pantalla.



6. Ahora, lanza una o más máquinas virtuales; En este laboratorio, estamos iniciando sesión en **Window Server 2016** y **Debian 9**.

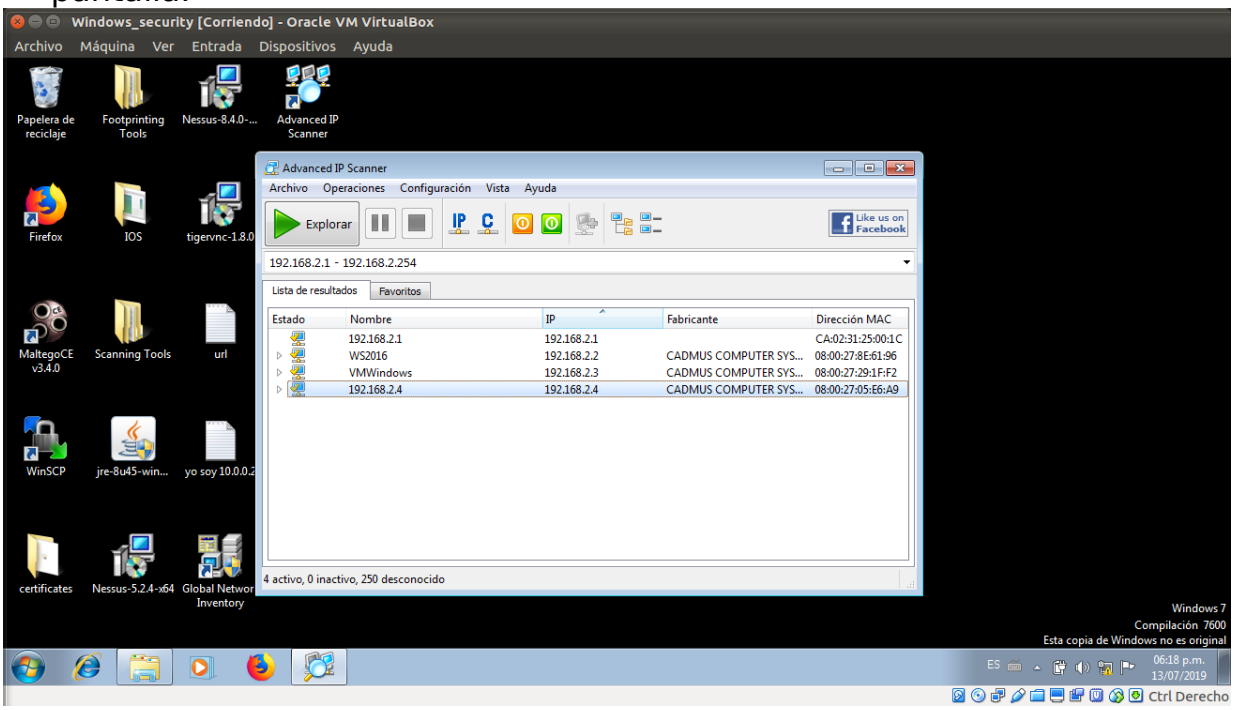
7. Vuelva a la máquina atacante (**Windows 7**) y especifique el rango de direcciones IP en el campo **Seleccionar rango**.

8. Haga clic en el botón **Explorar** para comenzar la exploración.



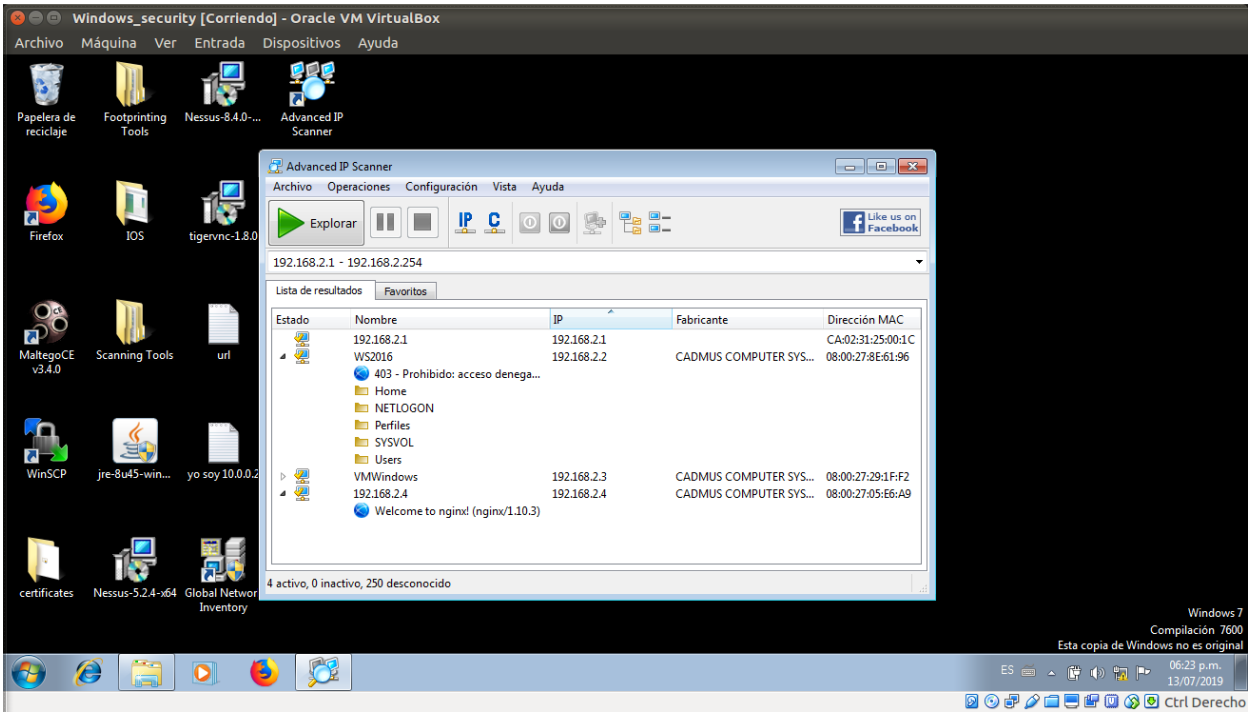
9. **Advanced IP Scanner** escanea todas las direcciones IP dentro del rango y muestra los resultados del escaneo**.**

10. Muestra el estado como vivo como se muestra en la siguiente captura de pantalla.

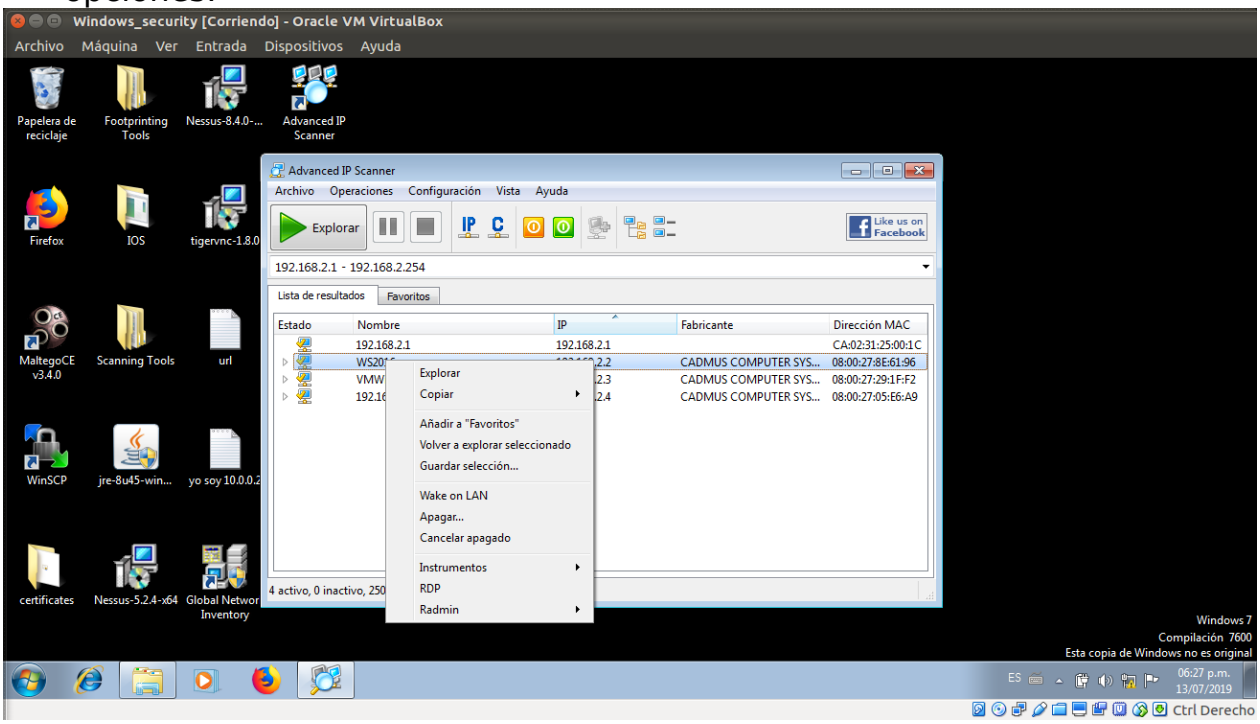


11. Ahora tiene la **dirección IP**, **el nombre**, **la dirección MAC** y la información del fabricante de la máquina víctima.

12. Haga clic en **Expandir todo** para ver las carpetas compartidas y los servicios que se ejecutan en la máquina víctima.



13. Haga **clic con el botón derecho** en cualquiera de las direcciones IP detectadas para ver Wake-On-Lan, shutdown, abort shutdown y otras opciones.



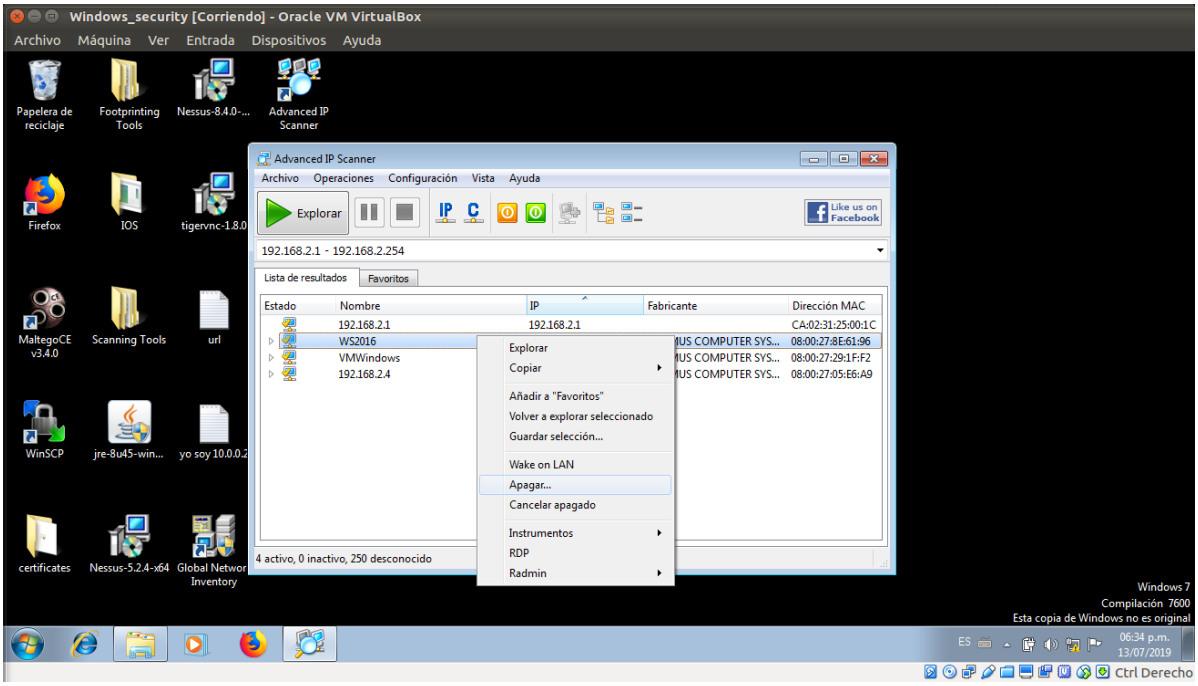
14. Con estas opciones, puede hacer ping, trazar rutas, transferir archivos, chatear, enviar un mensaje, conectarse a la máquina de la víctima de forma remota (usando Radmin), etc.

Nota: Para utilizar la opción Radmin, debe instalar el visor de Radmin, que puede descargar en www.radmin.com.

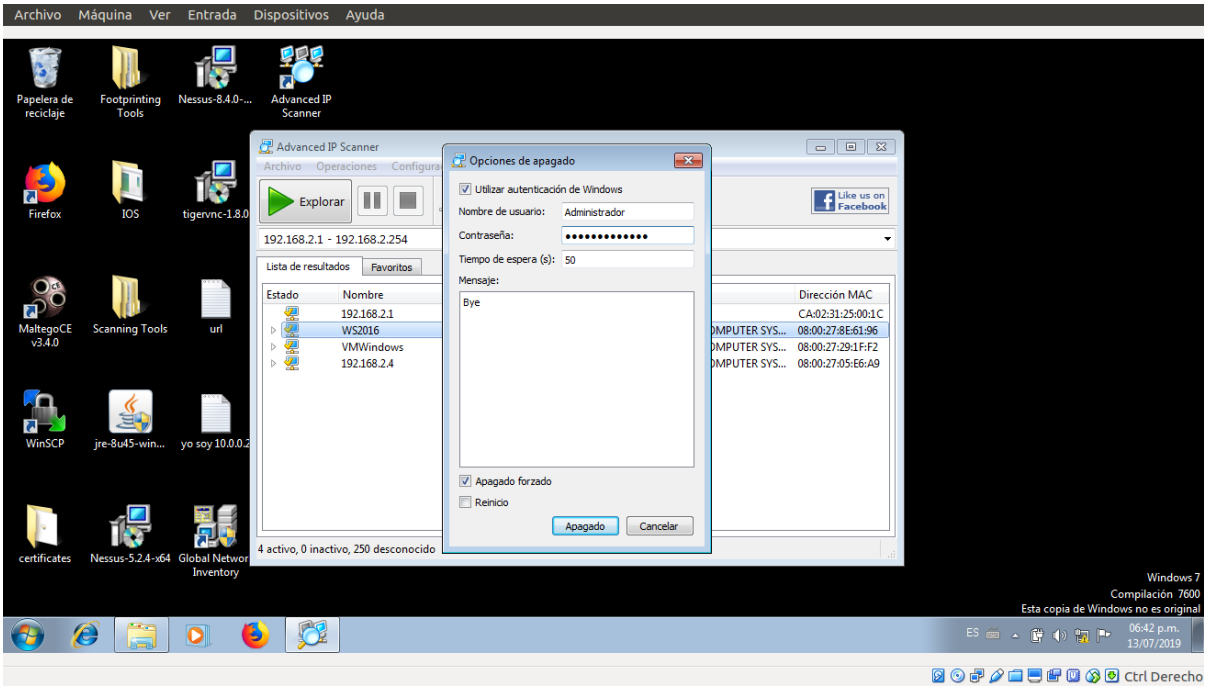
15. Un atacante también puede hacer uso de estas opciones y usar varias otras (por ejemplo, apagar una máquina remota) que se describen a continuación.

16. Puede forzar el apagado, el reinicio y el apagado de la máquina víctima seleccionada.

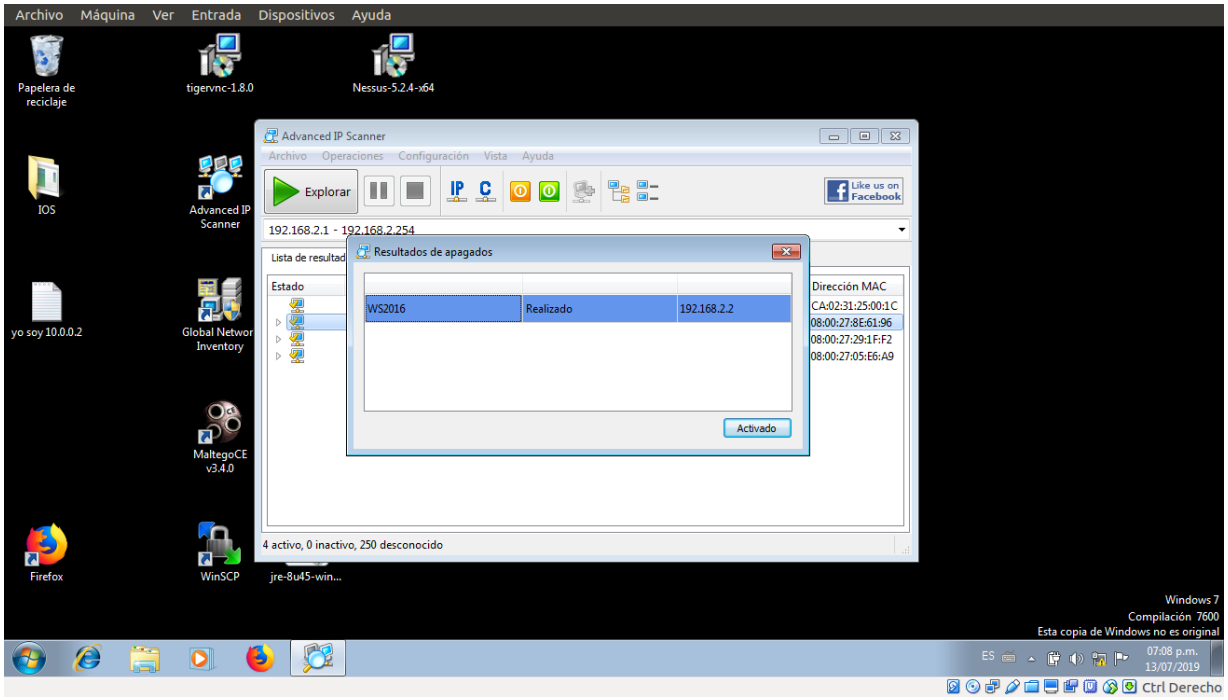
17. Haga clic con el botón derecho en 192.168.2.2 y seleccione Apagar.



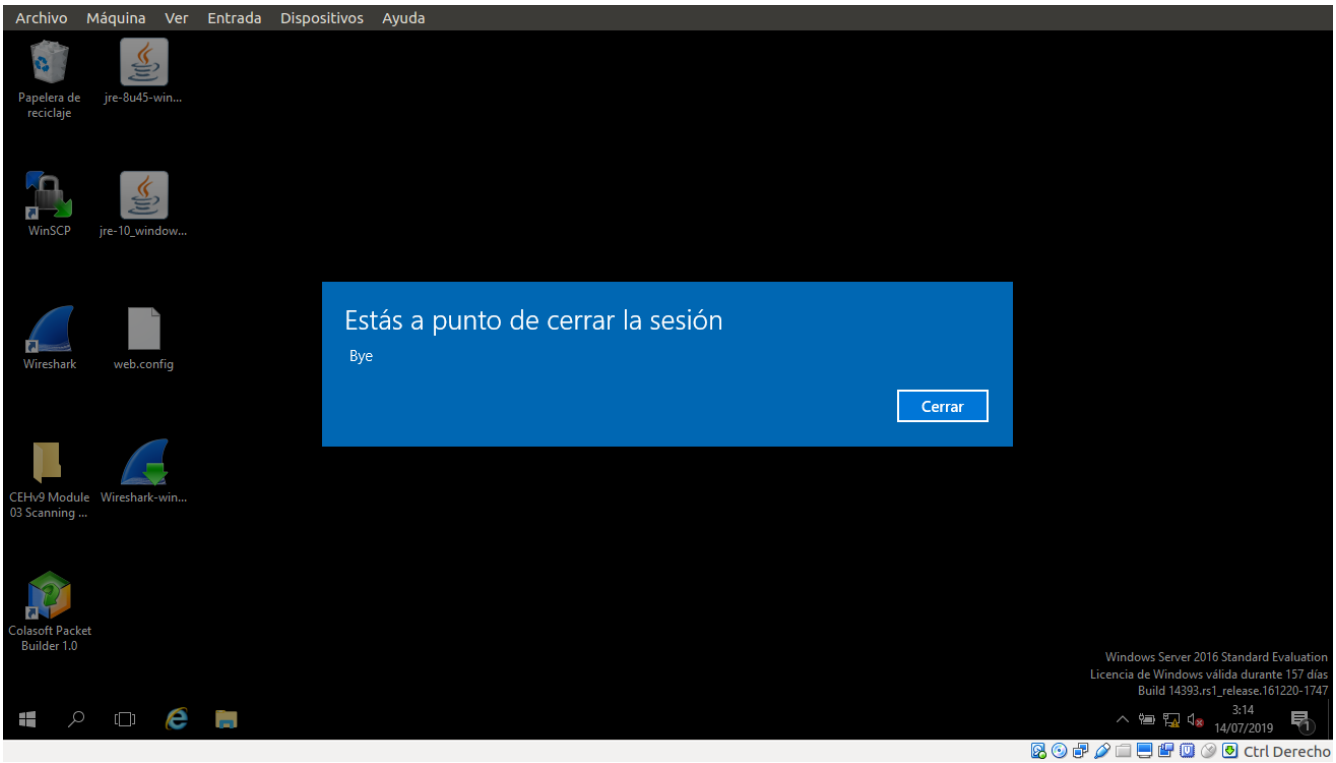
18. Se abre la ventana de opciones de apagado; establezca un T**iempo de espera** (aquí, 50 segundos) y haga clic en **Apagar** para apagar la máquina virtual.



19. Aparece la ventana emergente de resultados de apagado; haga clic en **Aceptar.**



20. La máquina víctima se apagará después del tiempo especificado**.**



21. Por lo tanto, un atacante también puede descubrir máquinas en una red y usar varias opciones para recuperar archivos compartidos, ver información relacionada con el sistema, etc.