



# Entendiendo el escaneo en red usando Nmap

*Nmap (Zenmap es la GUI oficial de Nmap) es una utilidad gratuita de código abierto (licencia) para la exploración de redes y auditorías de seguridad.*

## Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a aprender y entender cómo:

- Escanear una subred entera
- Rastrea todos los paquetes enviados y recibidos.
- Realizar un escaneo completo lento
- Crear un nuevo perfil para realizar un escaneo nulo
- Escanear puertos TCP y UDP
- Analizar los detalles del host y su topología.

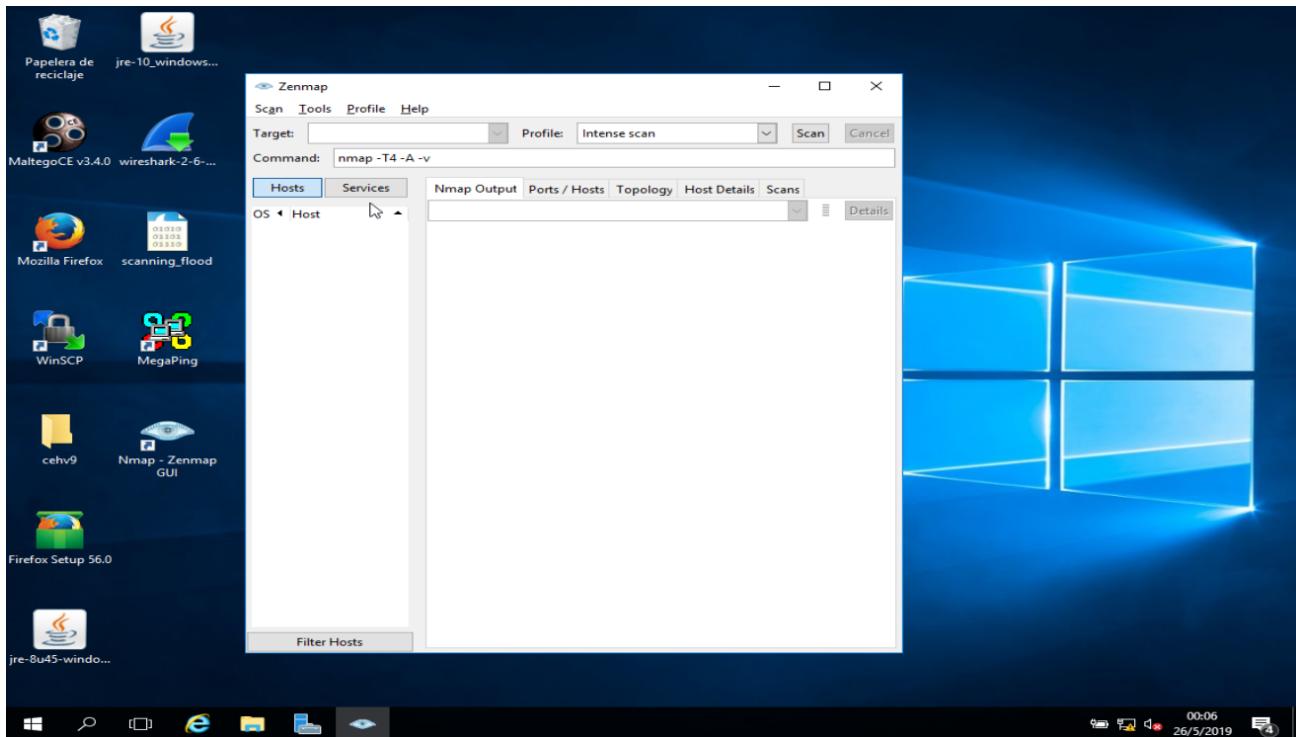
## Resumen de Nmap

Nmap es una utilidad utilizada para el descubrimiento de redes, la administración y la auditoría de seguridad. También se utiliza para tareas como el inventario de la red, la administración de los programas de actualización del servicio y el monitoreo del tiempo de actividad del host o del servidor.

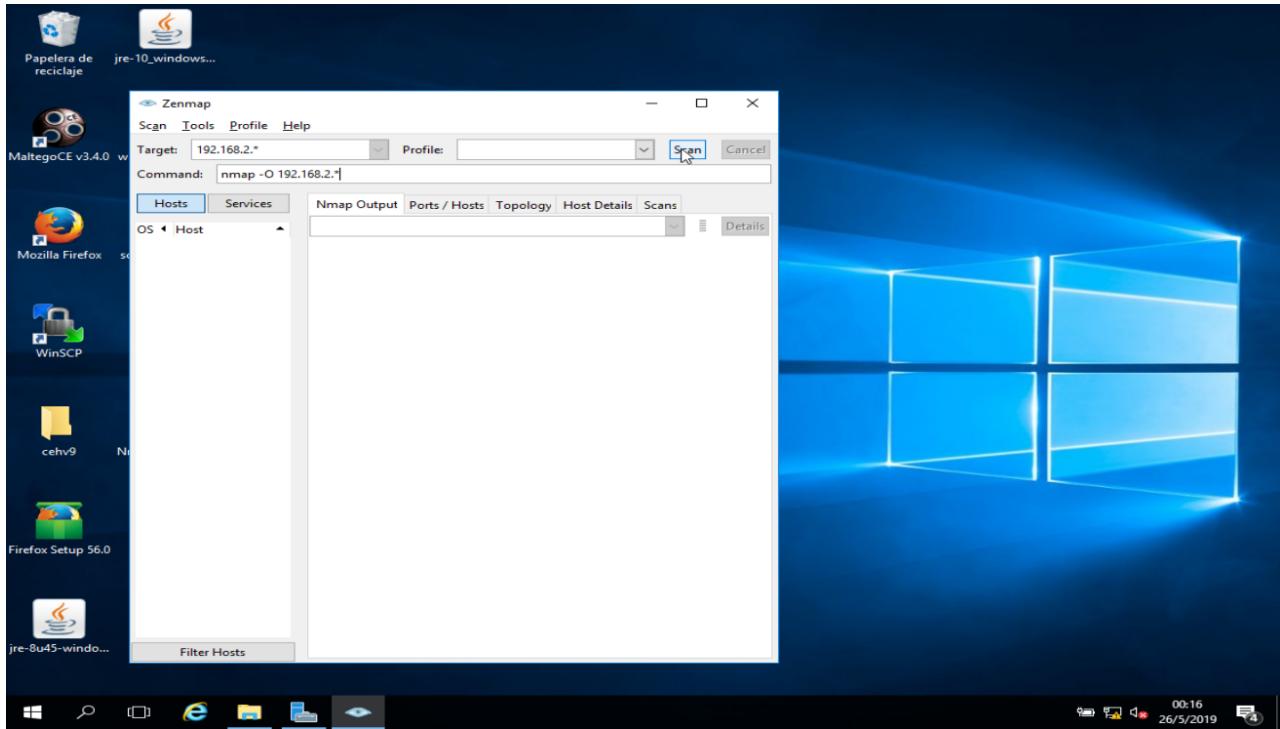
## Tareas del laboratorio

1. Inicie sesión en una o más máquinas virtuales. En esta tarea de laboratorio, hemos utilizado Debian 9, Windows 7, servidor Windows 2016.
2. Navega hasta el directory donde tengas el ejecutable de nmap y has doble clic en el archivo .exe

3. Cuando aparezca la ventana damos click en Iniciar
4. En la ventana de configuración de Nmap, haga clic en Acepto y siga los pasos de instalación para instalar Nmap usando todos los valores predeterminados.
5. En el momento de la instalación, aparece una ventana emergente de configuración de **WinPcap**. Si ya está instalada una versión superior de **WinPcap**, haga clic en **No** y siga los pasos de instalación guiados por el asistente para instalar Nmap.
6. Al finalizar la instalación, inicie la aplicación **Nmap - Zenmap GUI** desde la pantalla de aplicaciones. Puede presionar la tecla "Windows" para acceder a la pantalla principal de Windows para el servidor 2016.
7. La GUI de **Nmap - Zenmap** aparece con el perfil de escaneo intenso configurado de forma predeterminada.

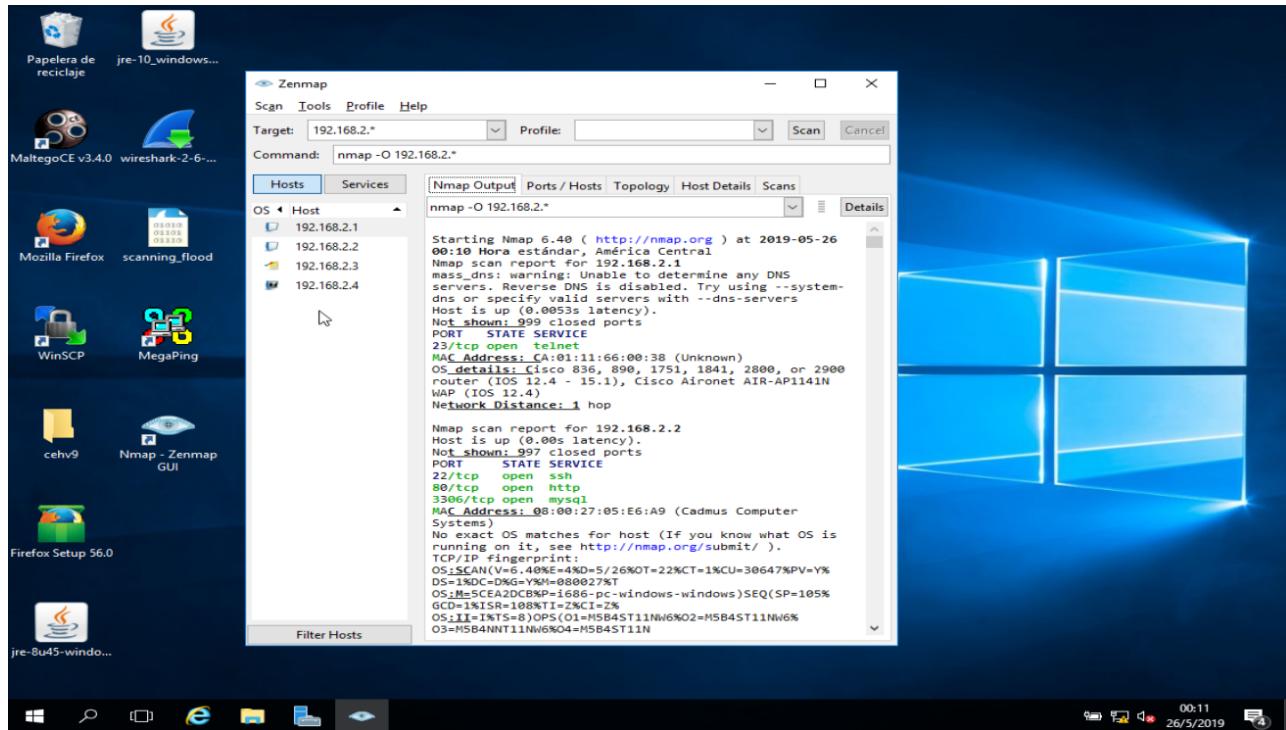


8. En el campo **Comando**, escriba el comando nmap -O seguido del rango de direcciones IP. En este laboratorio, es 192.168.2.0. Al proporcionar el comodín "\*", puede escanear una subred completa o rango de IP con Nmap para descubrir hosts activos.
9. Haga clic en **Escanear** para comenzar a escanear las máquinas virtuales

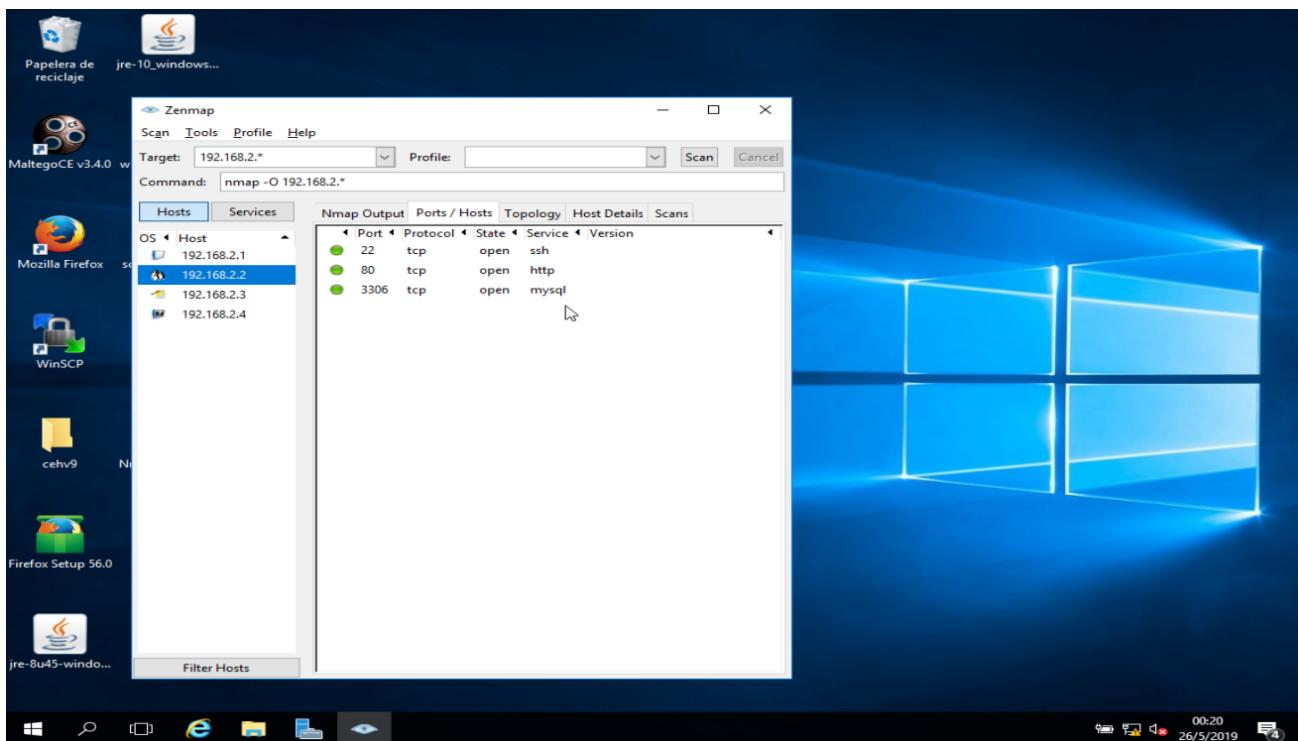


10. Nmap escanea toda la red y muestra información de todos los hosts que se escanearon, junto con los puertos abiertos, el tipo de dispositivo, los detalles del sistema operativo, etc.

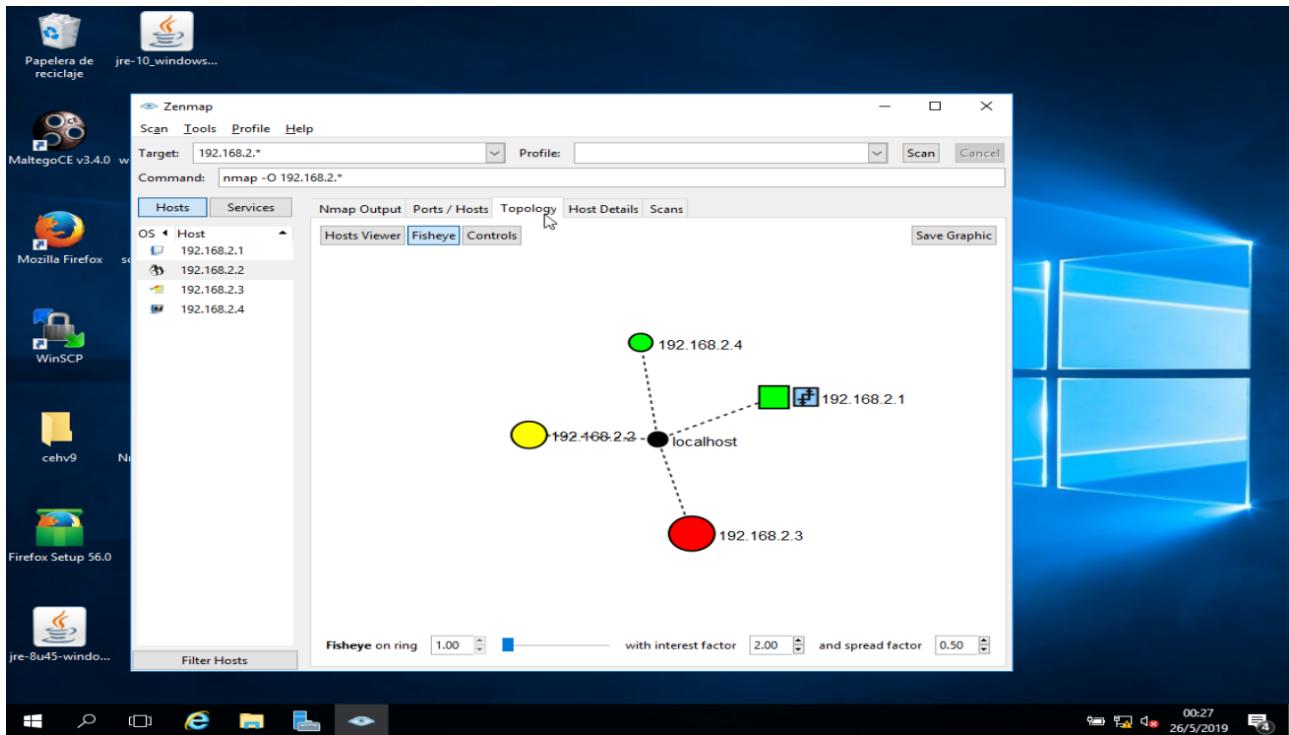
11. Desplácese hacia abajo en la ventana o seleccione la dirección IP de un host de la lista de hosts en el panel izquierdo para ver sus detalles.



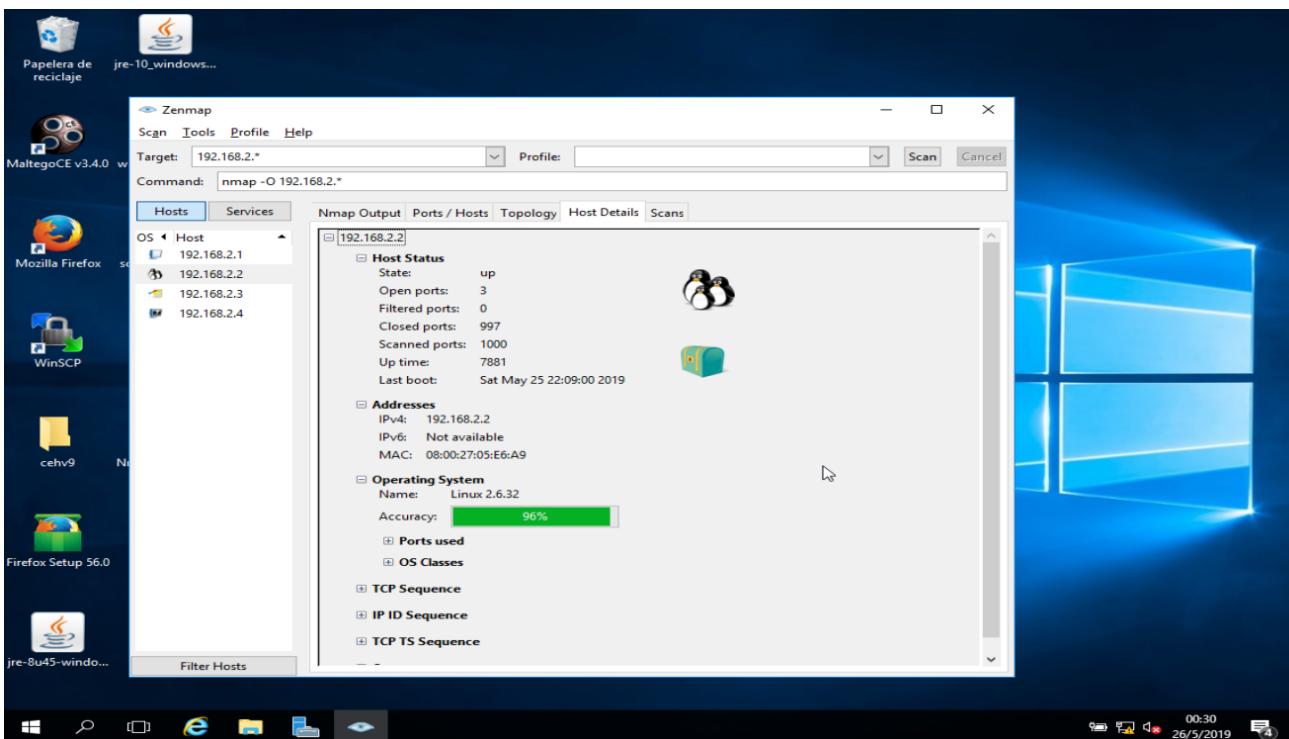
12. Haga clic en la pestaña **Puertos / Hosts** y elija la dirección IP de un host (aquí se seleccionó **192.168.2.2**) en el panel izquierdo para ver todos los puertos abiertos asociados con el host seleccionado.



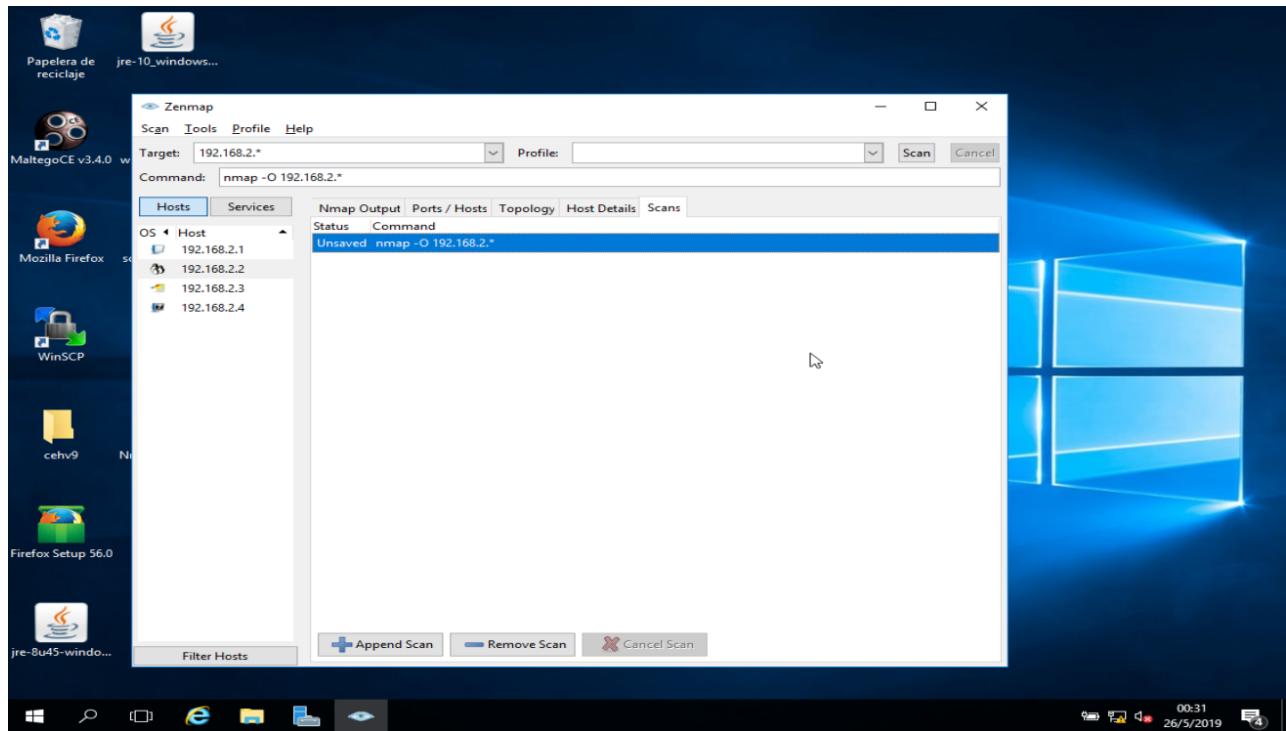
13. Un atacante podría intentar establecer una conexión a través de cualquiera de estos puertos abiertos explotando cualquier vulnerabilidad (si se encuentra) en un servicio en ejecución.
14. Haga clic en la pestaña **Topología** para ver la topología de la red de destino que contiene la dirección IP de destino.
15. Haga clic en la opción **Ojo de pez** para ver la topología de forma clara.



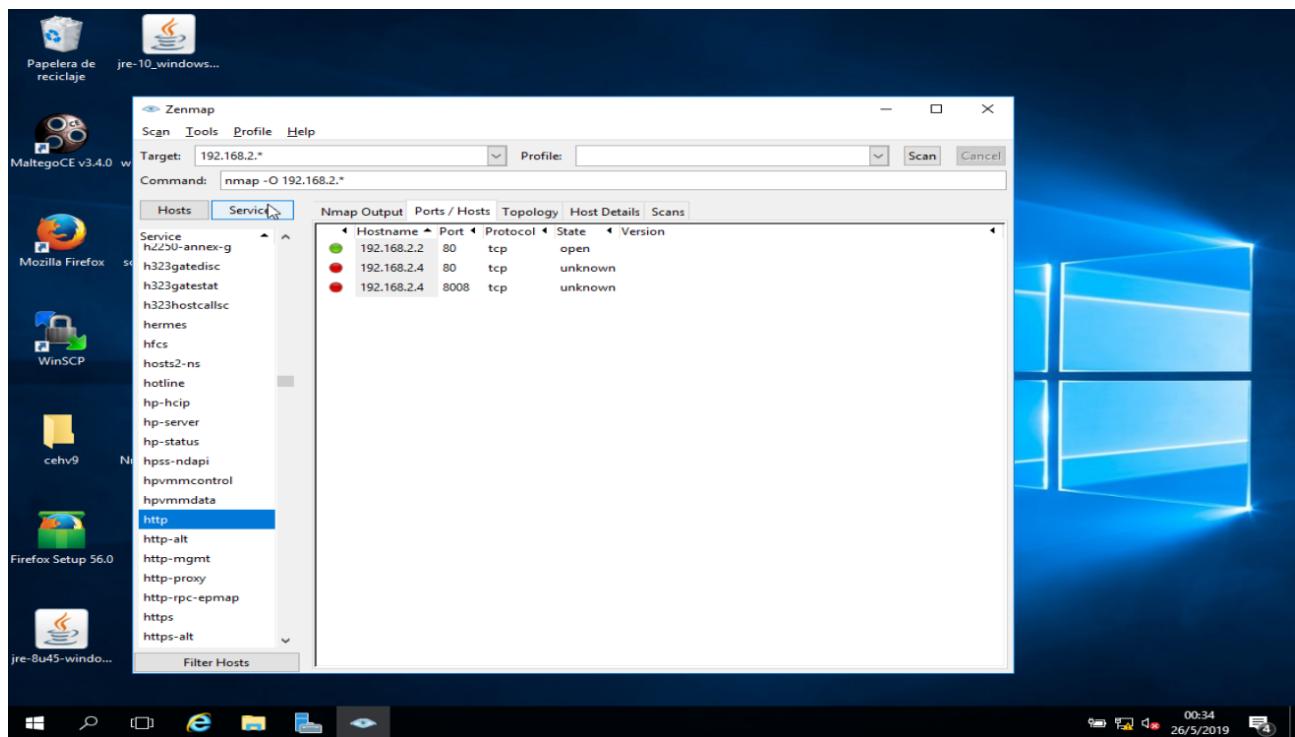
16. Haga clic en la pestaña **Detalles del host** y seleccione la dirección IP de un host (aquí 192.168.2.2) para ver los detalles del host que se descubrió durante la exploración.



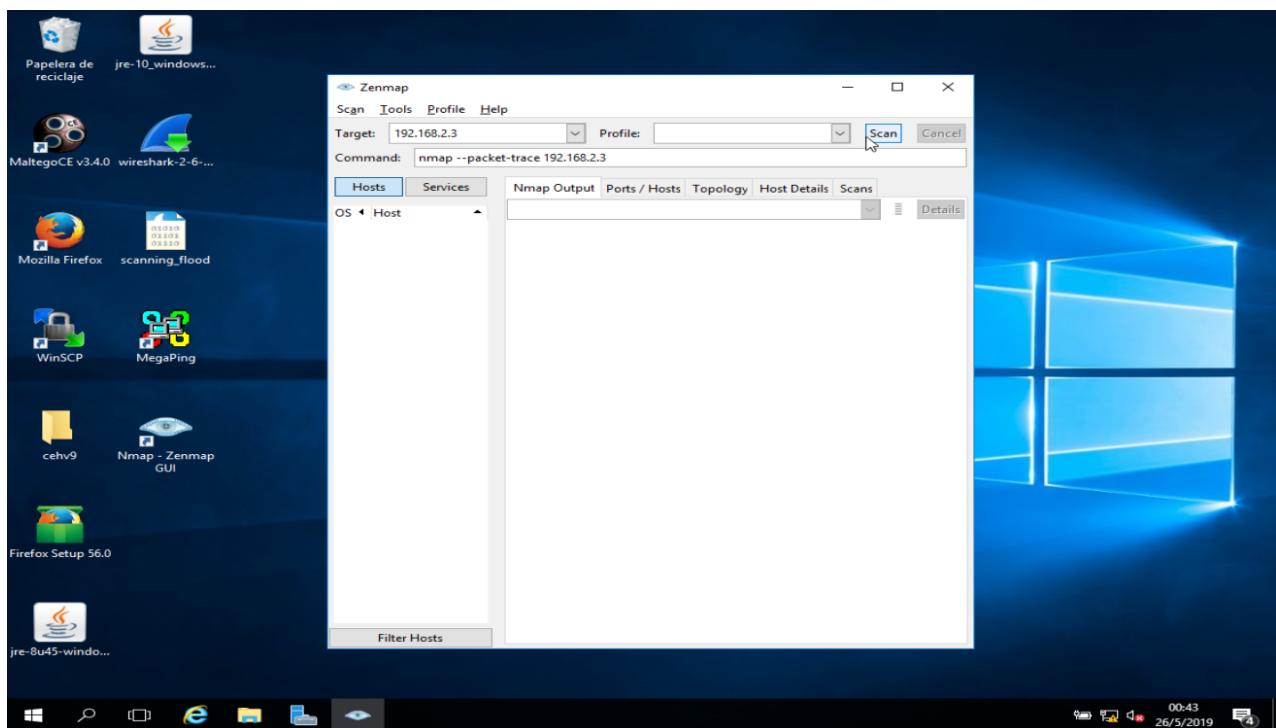
17. Haga clic en la pestaña **Exploraciones** para ver el estado de la exploración.



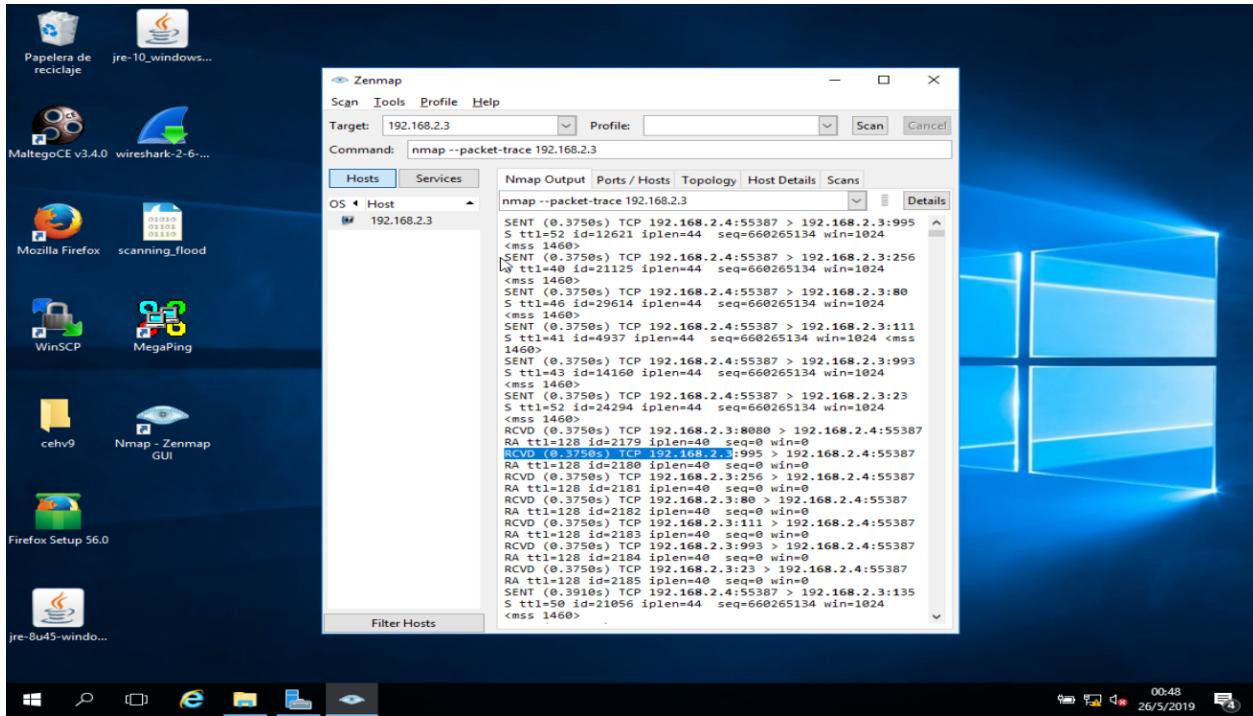
18. Haga clic en la pestaña **Servicios** y seleccione cada servicio (aquí se ha elegido http) para enumerar todos los puertos en los que el servicio está ejecutando su estado (abierto / cerrado / desconocido), versión, etc.



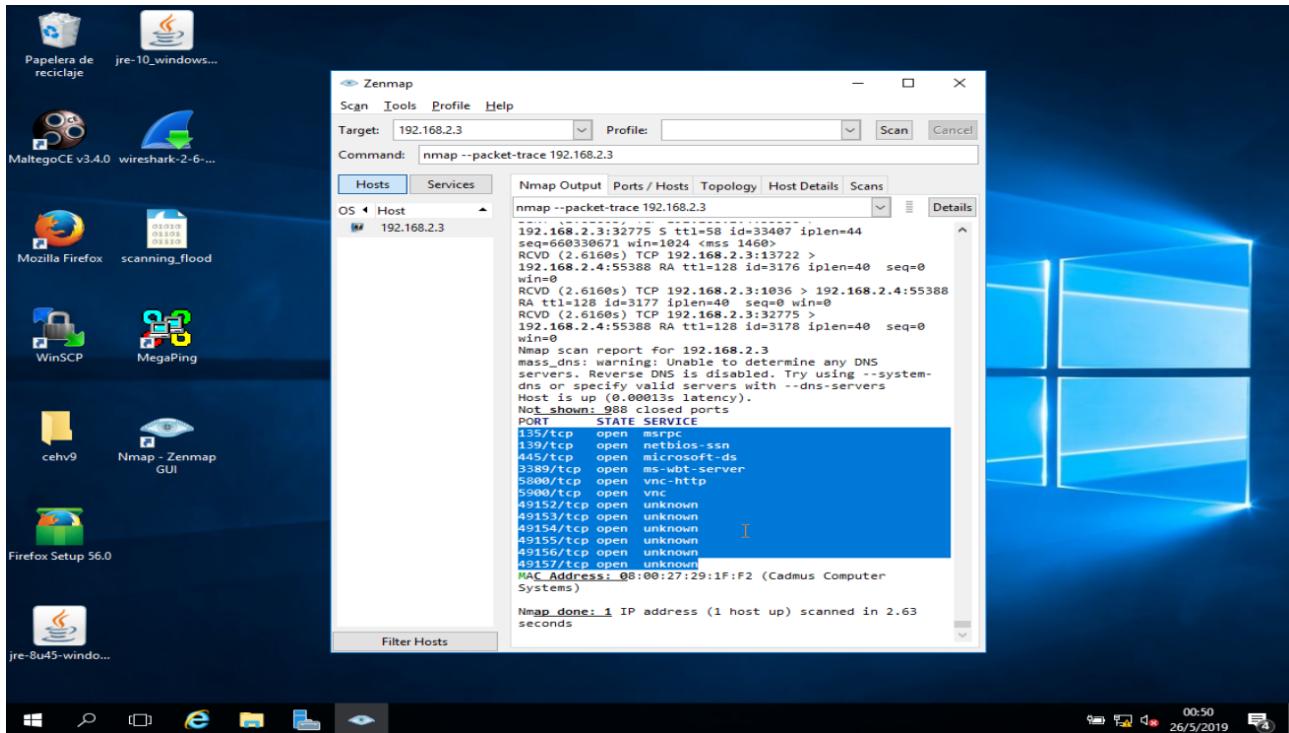
19. Una vez que se realiza la exploración, finalice la exploración y salga de la aplicación Nmap.
20. Inicia Nmap desde la pantalla de **aplicaciones**.
21. En el campo **Comando**, escriba el comando nmap --packet-trace seguido de la dirección IP de la máquina de destino (Windows 7 [192.168.2.3]).
22. Está realizando un inventario de red para la máquina virtual.
23. Haga clic en **Escanear** para comenzar a escanear la máquina virtual.



24. Al emitir el comando **--packet-trace**, Namp envía paquetes a la máquina deseada y recibe paquetes en respuesta a los paquetes enviados. Imprime un resumen del paquete que envía y recibe.
25. La siguiente captura de pantalla muestra los paquetes enviados desde el host al destino y los paquetes recibidos del destino al host que se muestran en la pestaña Salida de Nmap en Nmap:

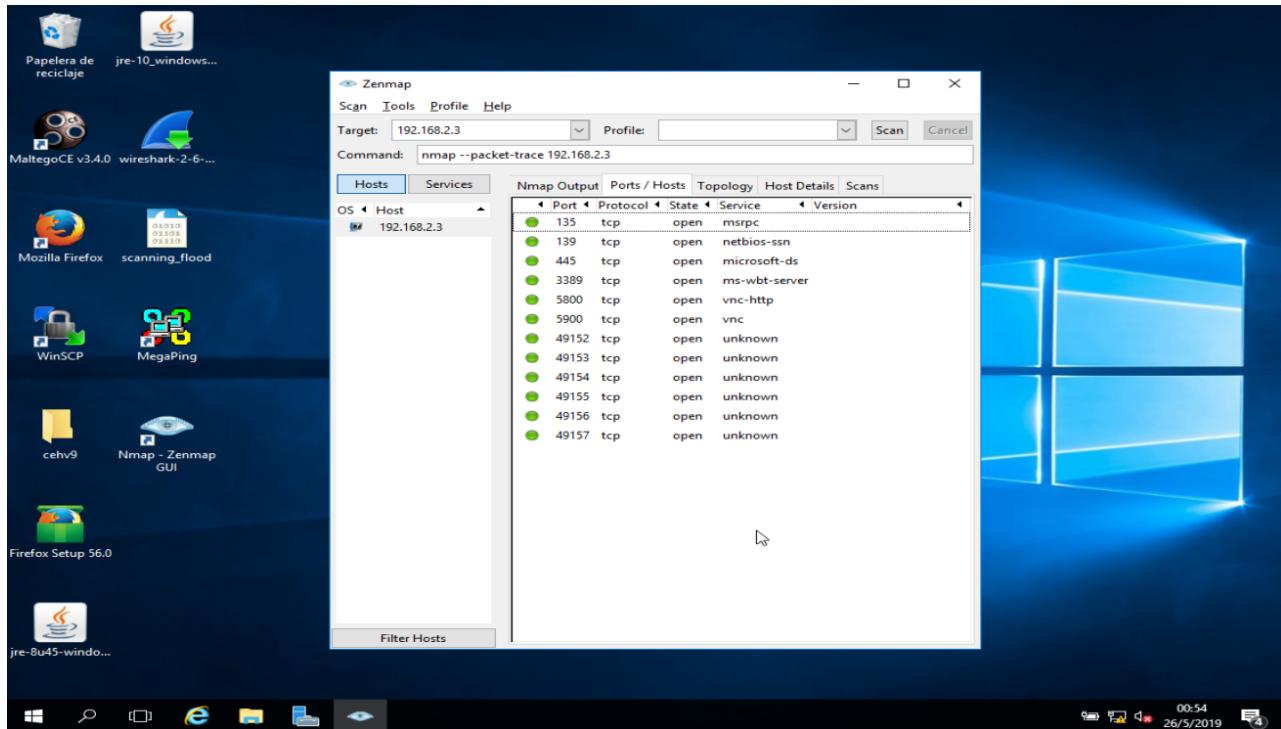


26. Desplácese hacia abajo de la ventana para ver los puertos TCP abiertos.



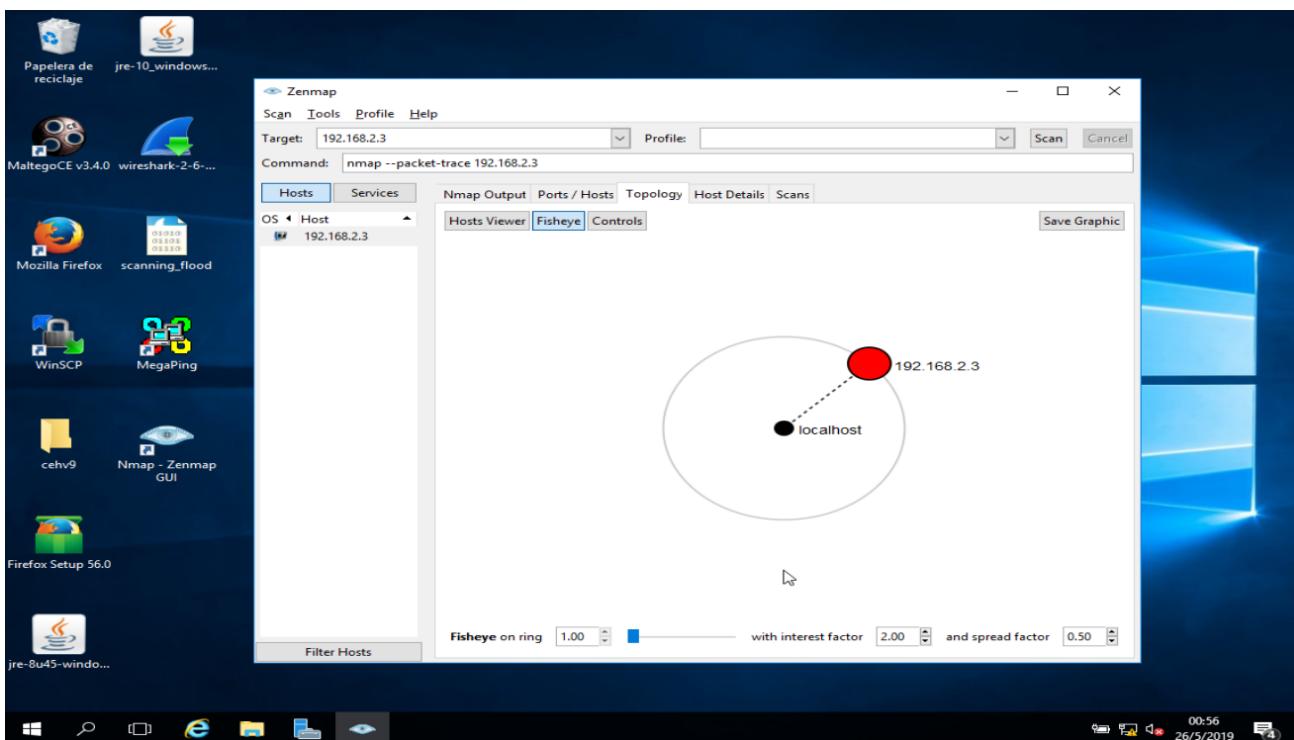
27. Haga clic en la pestaña **Puertos / Hosts** para mostrar más información sobre los resultados del análisis.

28. Nmap muestra el **Puerto**, el **Protocolo**, el **Estado**, el **Servicio** y la **Versión** de la exploración. Aquí, como puede observar, se ha encontrado más número de puertos abiertos en comparación con el análisis anterior.

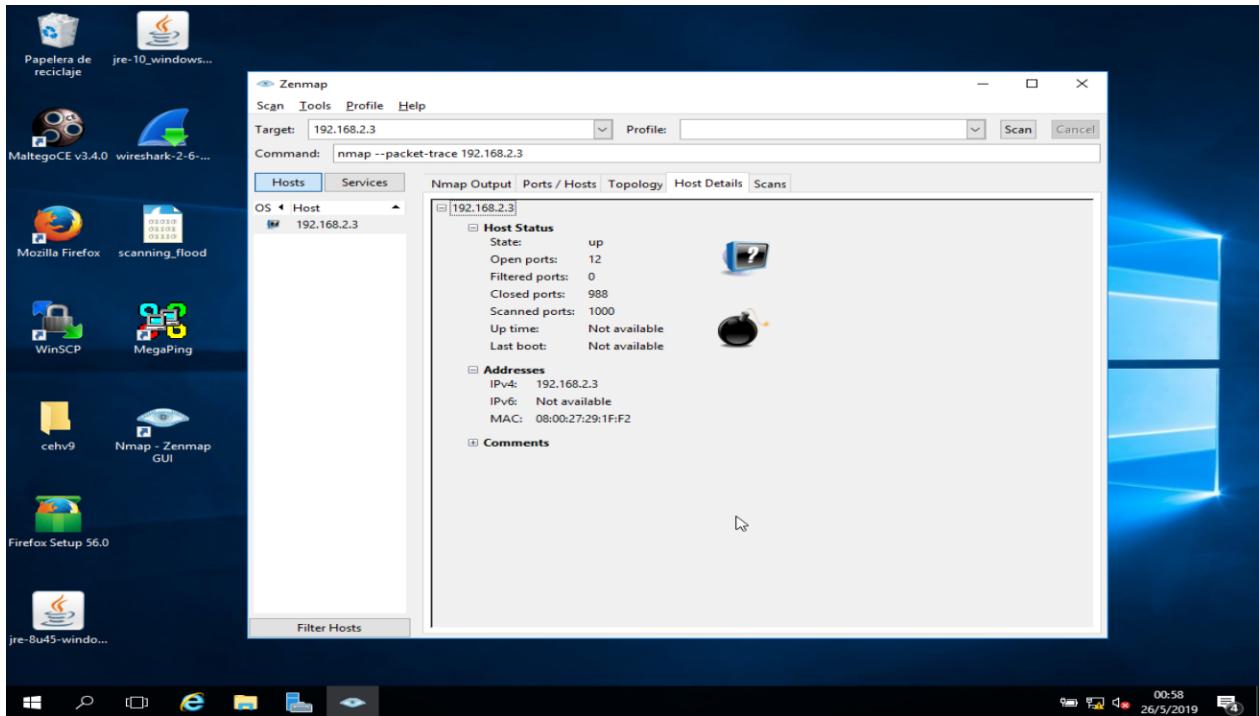


29. Haga clic en la pestaña **Topología** para ver la topología de la red de destino que contiene la dirección IP proporcionada.

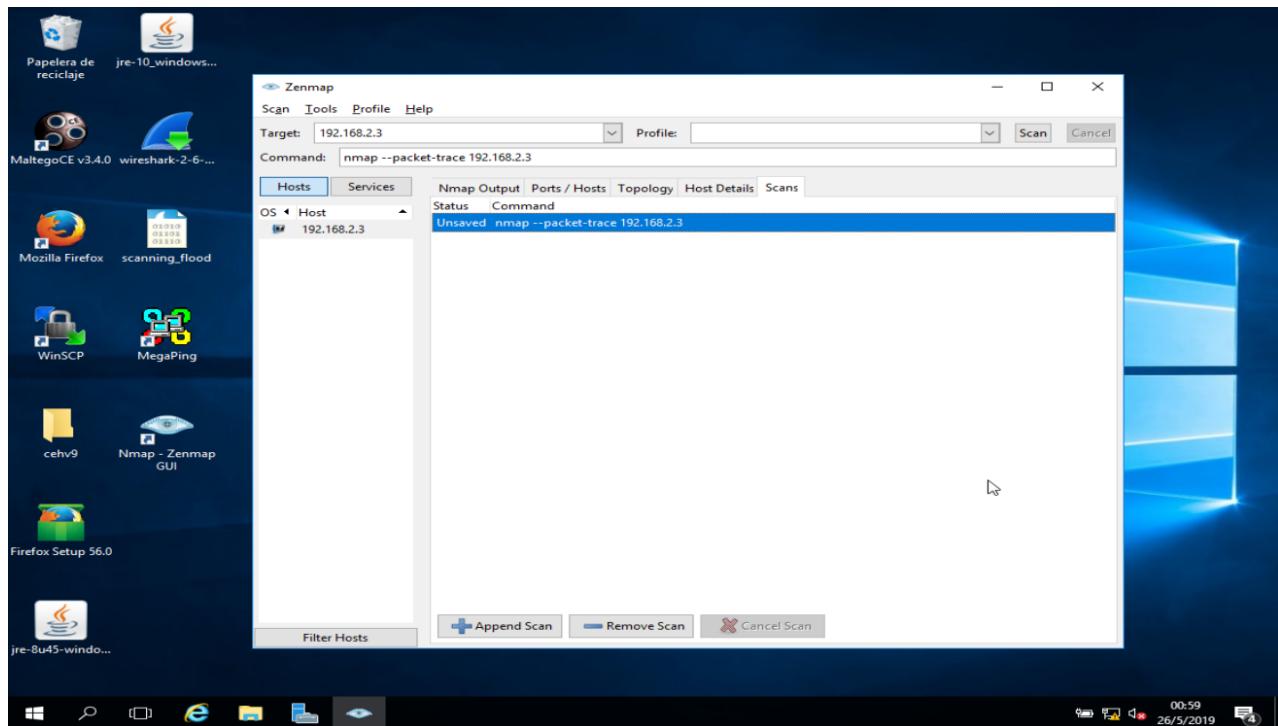
30. Haga clic en la opción **Ojo de pez** para ver la topología de forma clara.



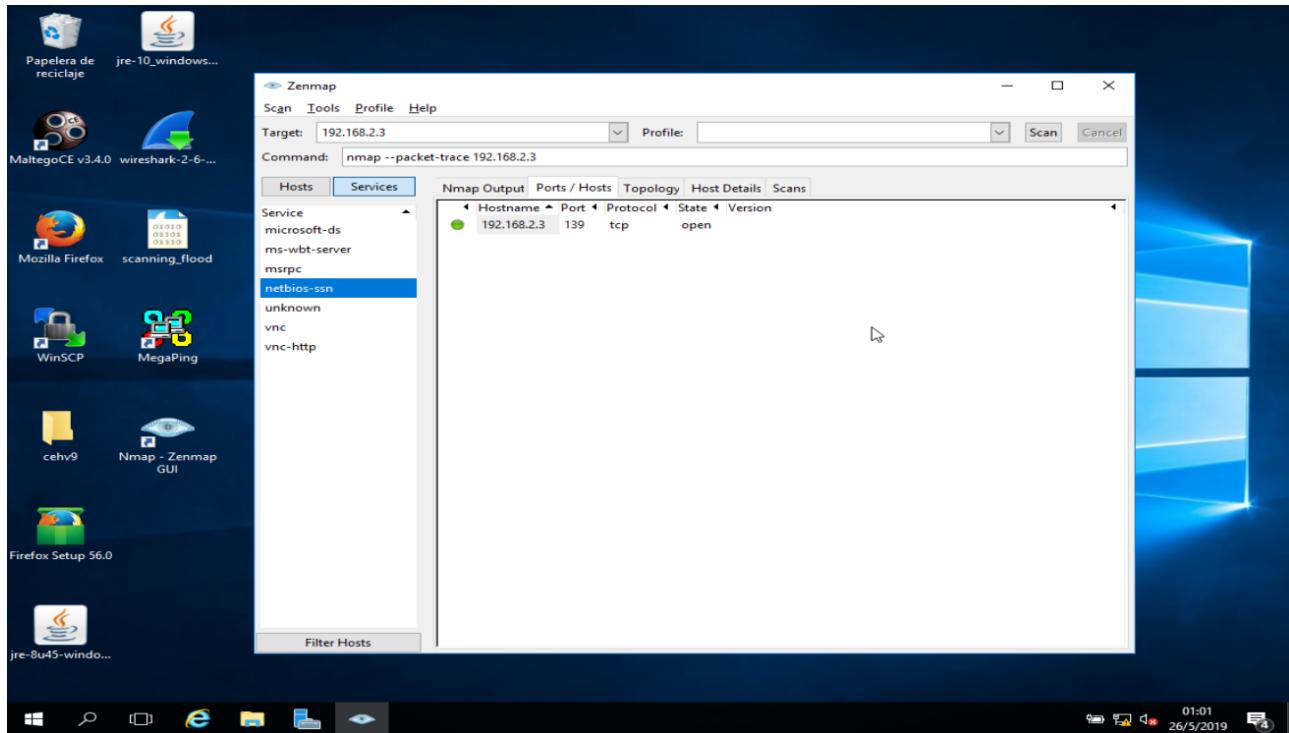
31. De la misma manera, haga clic en la pestaña **Detalles del host** para ver los detalles de todos los hosts descubiertos durante el perfil intenso.



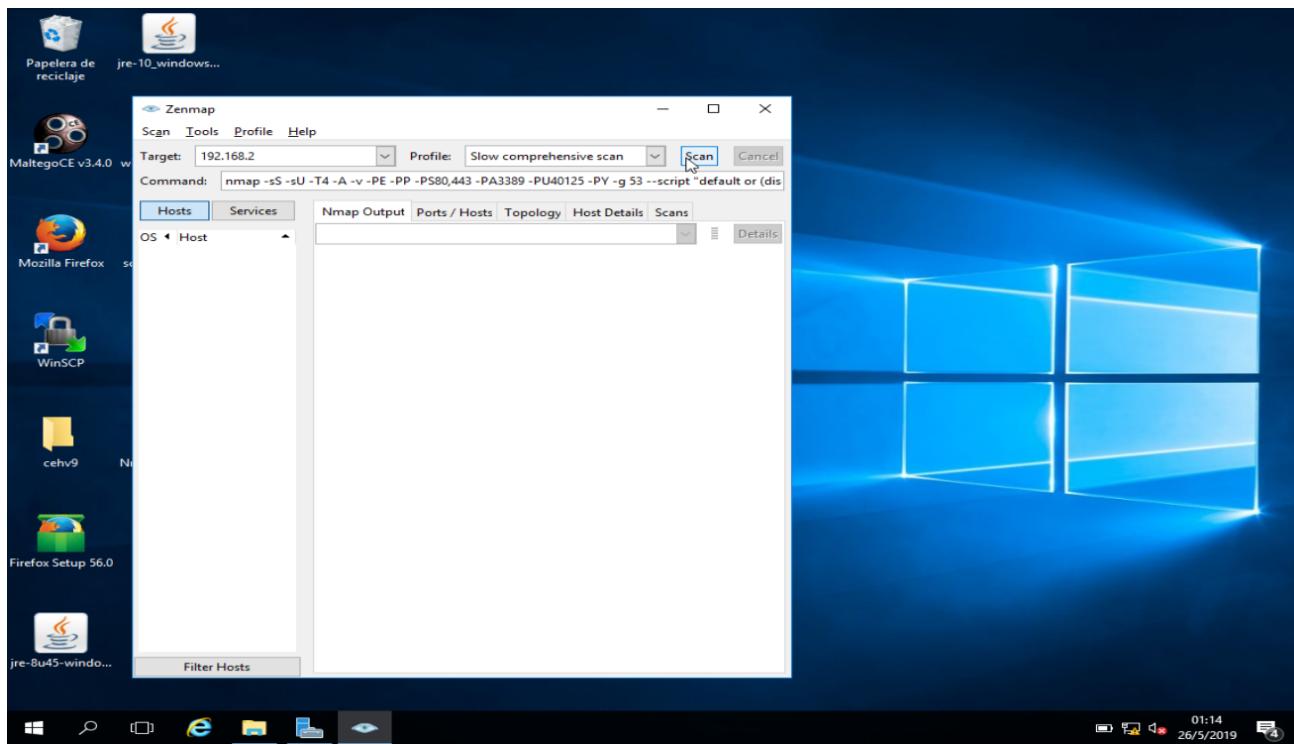
32. Haga clic en la pestaña **Exploraciones** para ver el estado de la exploración y el comando utilizado.



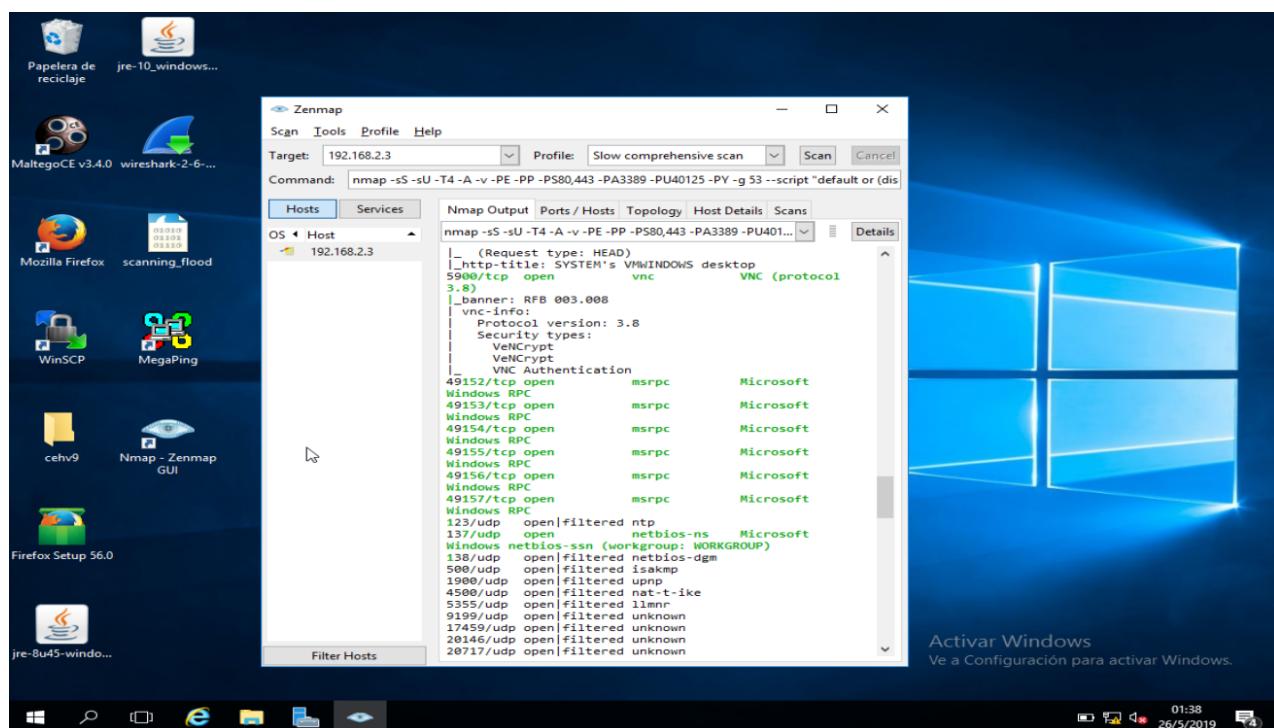
33. Haga clic en la pestaña **Servicios** ubicada en el panel derecho de la ventana. Esta pestaña muestra la lista de servicios.



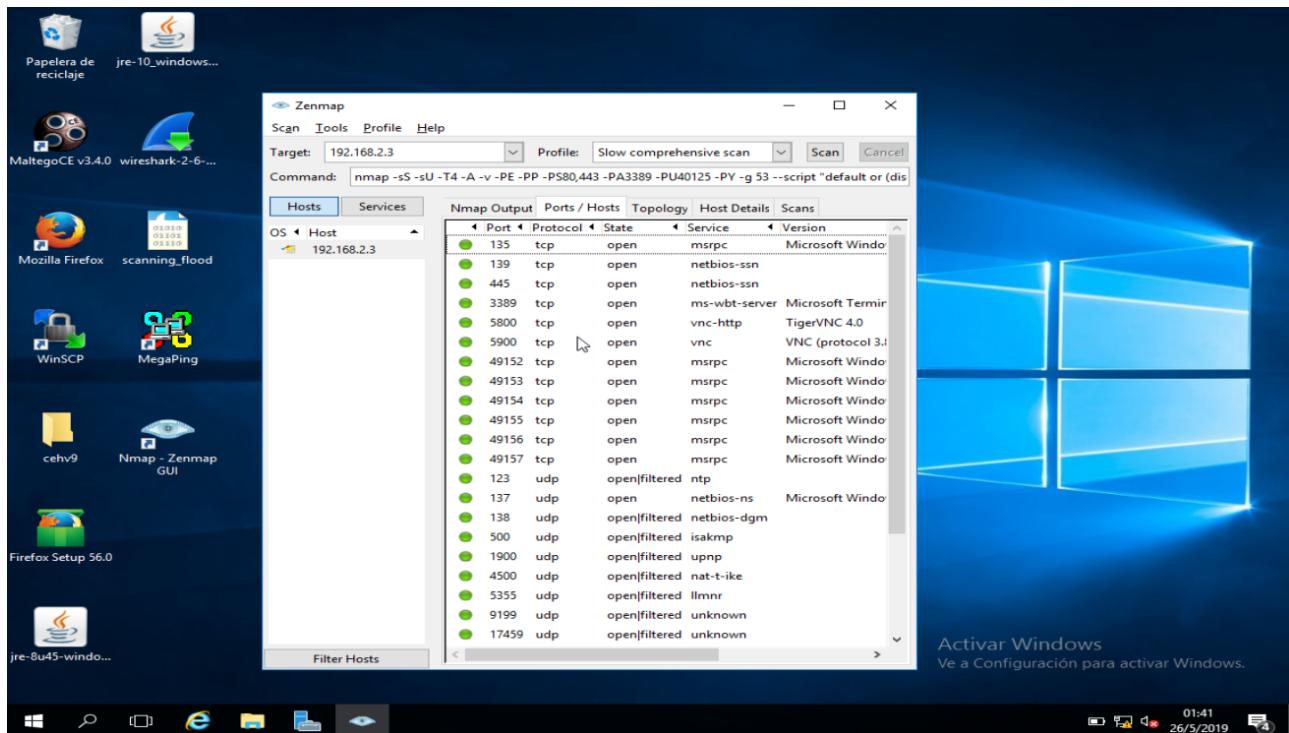
34. Un atacante usa cualquiera de estos servicios y sus puertos abiertos para ingresar a la red / host objetivo y establecer una conexión.
35. Una vez que se realiza la exploración, puede terminar Namp.
36. El escaneo lento y completo utiliza tres protocolos diferentes: TCP, UDP y SCTP tambien ayuda a determinar qué sistema operativo, servicios y versiones está ejecutando el host de acuerdo con los servicios TCP y UDP más comunes.
37. Es simplemente un escaneo intenso que utiliza el protocolo UDP además de algunas opciones de escaneo más. esta exploración se realiza en un intento de rastrear las máquinas en una red, incluso si están configuradas para bloquear solicitudes de ping.
38. Inicia Nmap desde la pantalla de aplicaciones.
39. Ingrese la dirección IP de **Windows 7** (192.168.2.3) en el campo **Destino**, seleccione Exploración lenta en la lista desplegable **Perfil** y haga clic en **Explorar**.



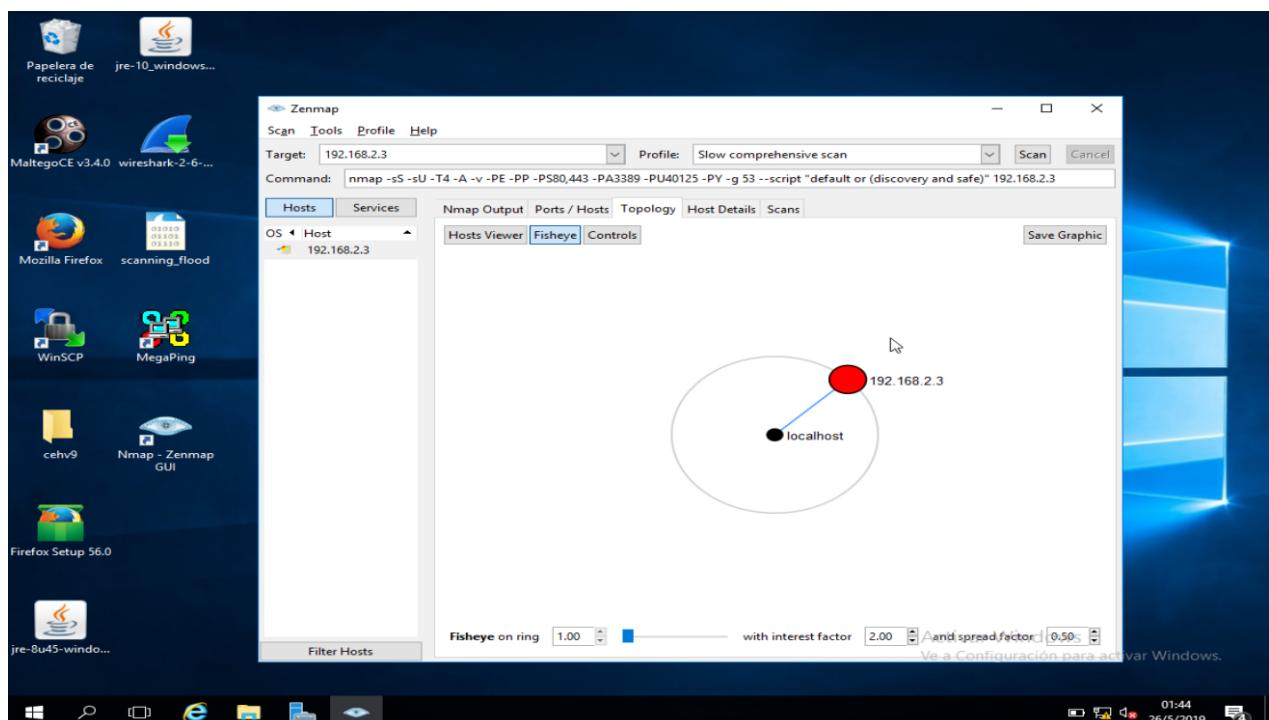
40. Nmap escanea la dirección IP de destino con un **escaneo lento y completo** y muestra el resultado del escaneo en la pestaña Salida de Nmap.



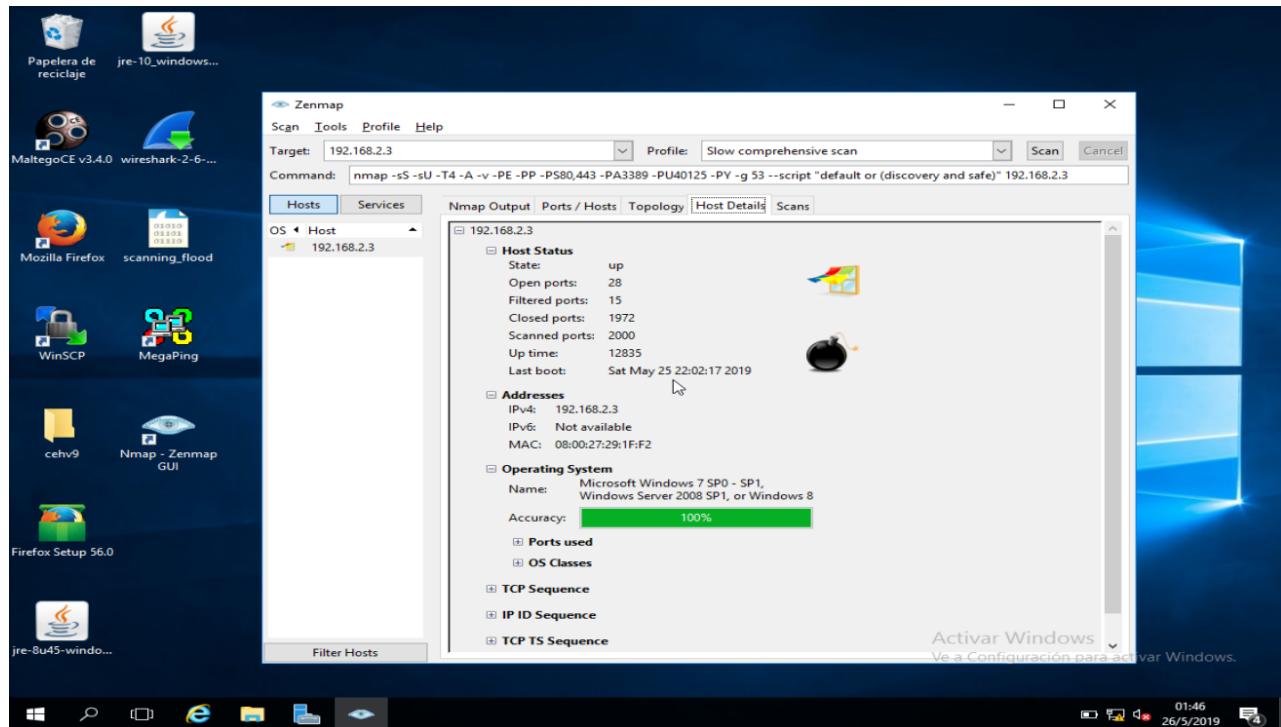
41. Haga clic en la pestaña **Puertos / Hosts** para mostrar más información sobre los resultados del análisis. Nmap emplea diversas técnicas de escaneo utilizando el escaneo lento y completo, y muestra más puertos abiertos.
42. Namp muestra los puertos, el protocolo, el estado, el servicio y la versión de la exploración.



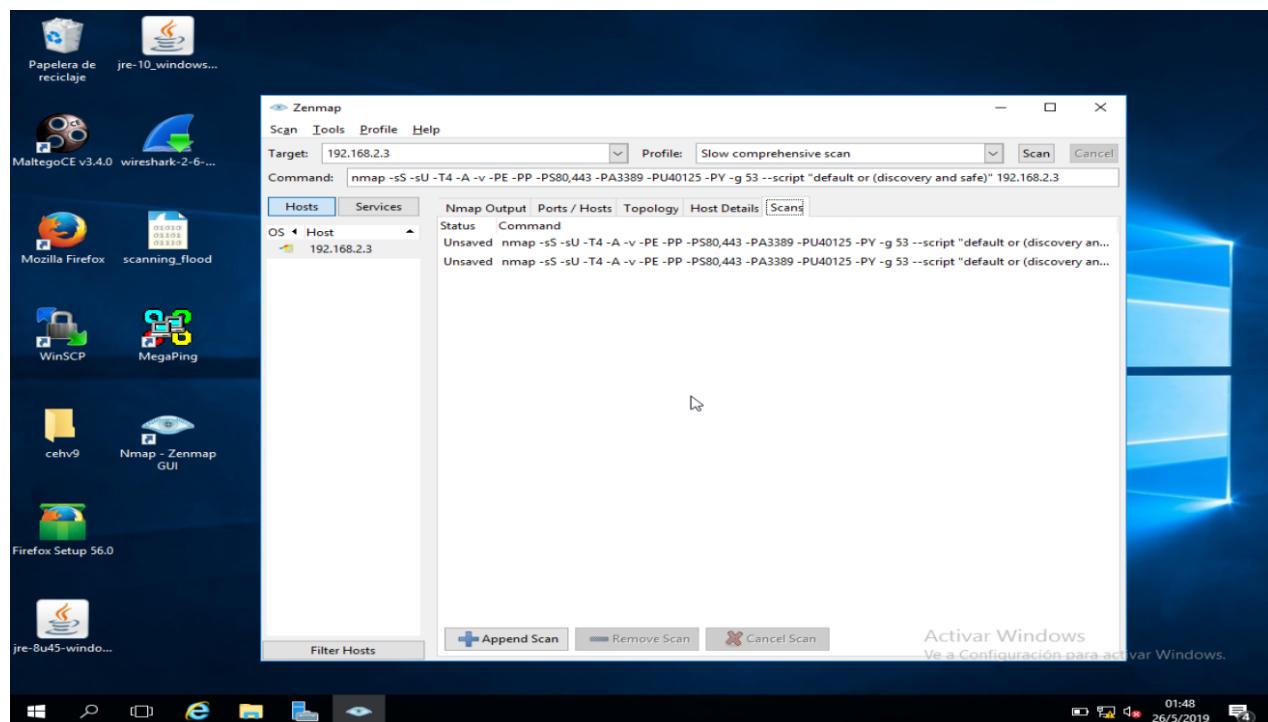
43. De la misma manera, haga clic en la pestaña **Topología** para ver la topología de la dirección IP de destino en el perfil de escaneo.



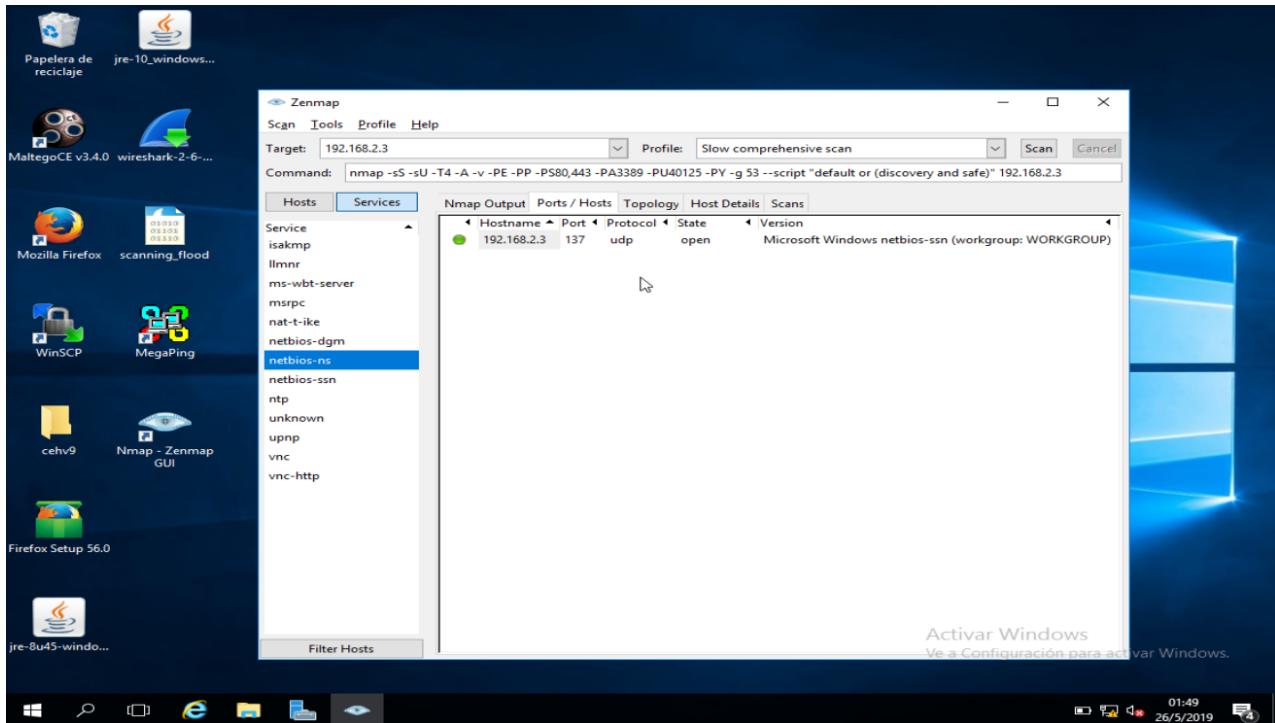
44. Haga clic en la pestaña **Detalles del host** para ver los detalles de todos los hosts descubiertos durante el intenso perfil.



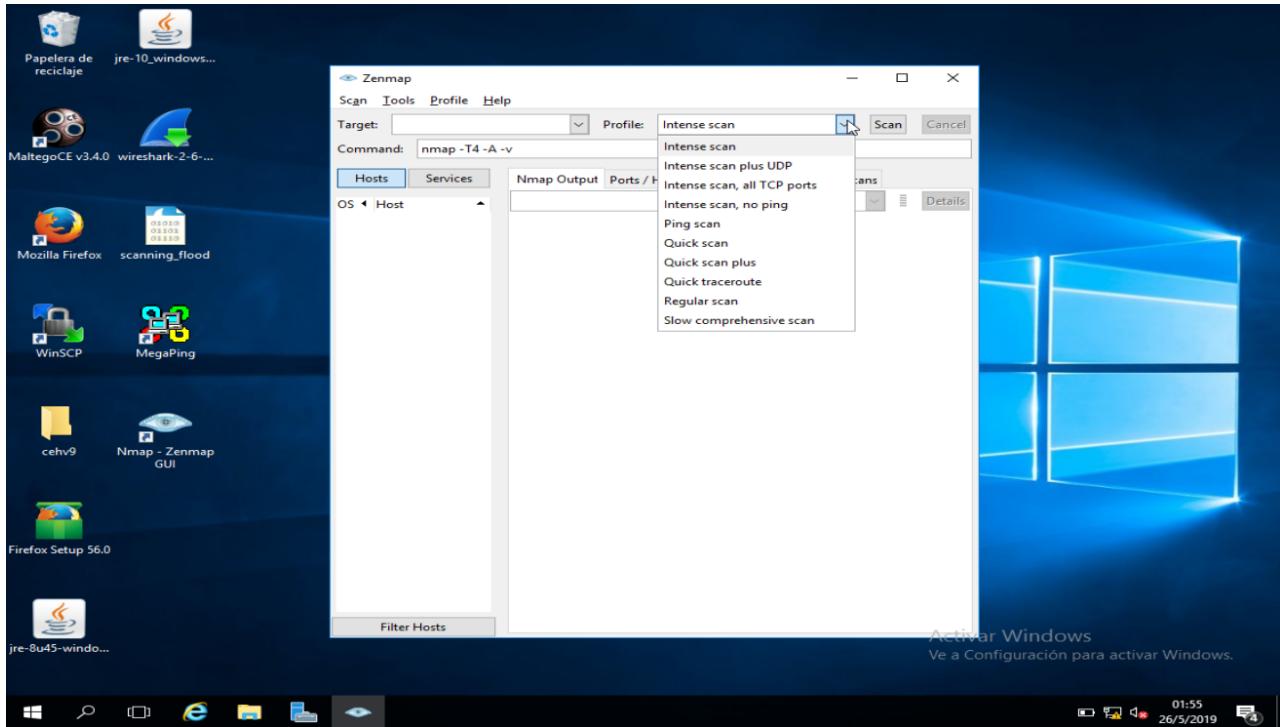
45. Haga clic en la pestaña **Exploraciones** para ver el estado de la exploración y el comando utilizado.



46. Haga clic en la pestaña **Servicios** ubicada en el panel derecho de la ventana. Esta pestaña muestra la lista de servicios.

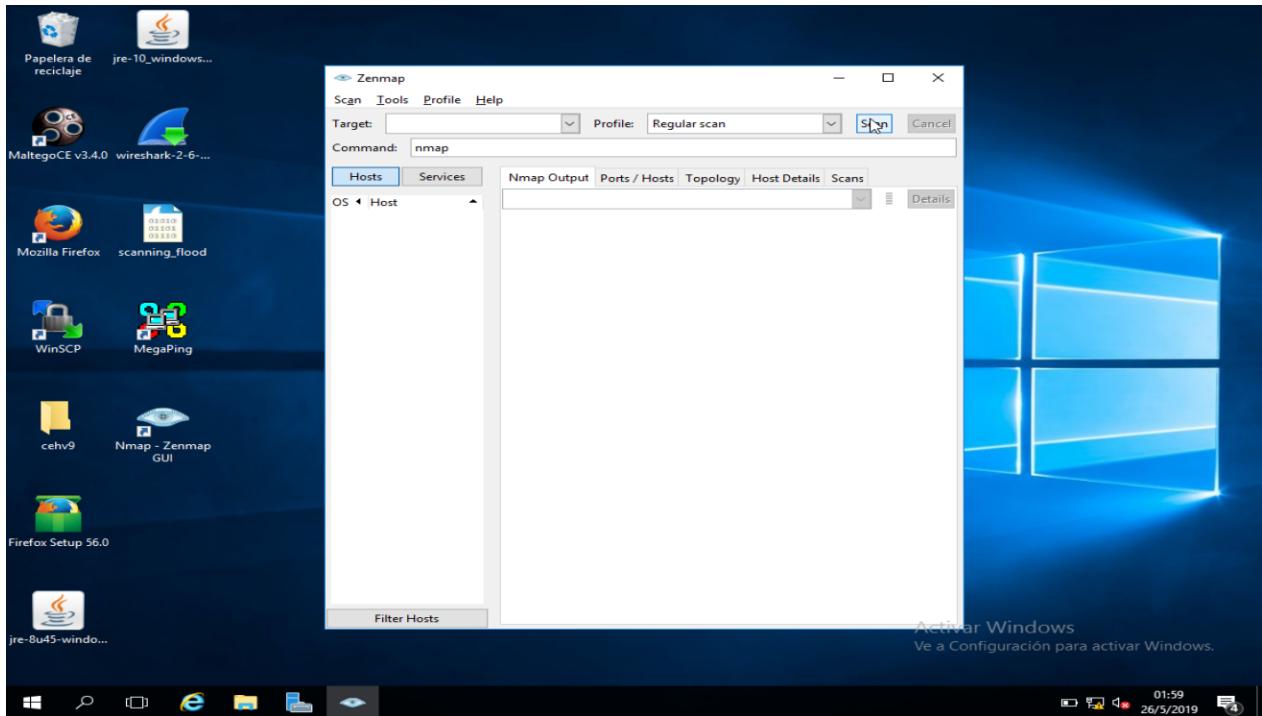


47. Un atacante usa cualquiera de estos servicios y sus puertos abiertos para ingresar a la red / host objetivo y establecer una conexión.
48. Una vez que se realiza la exploración, puede terminar la exploración.
49. Además de las exploraciones presentadas anteriormente, también puede realizar otras exploraciones como la exploración SYN, exploración XMAS, exploración de bandera ACK, etc., en un intento por descubrir máquinas y sus puertos y servicios abiertos en una red.
50. También puede elegir los perfiles de escaneo predeterminados disponibles en Nmap para escanear una red.

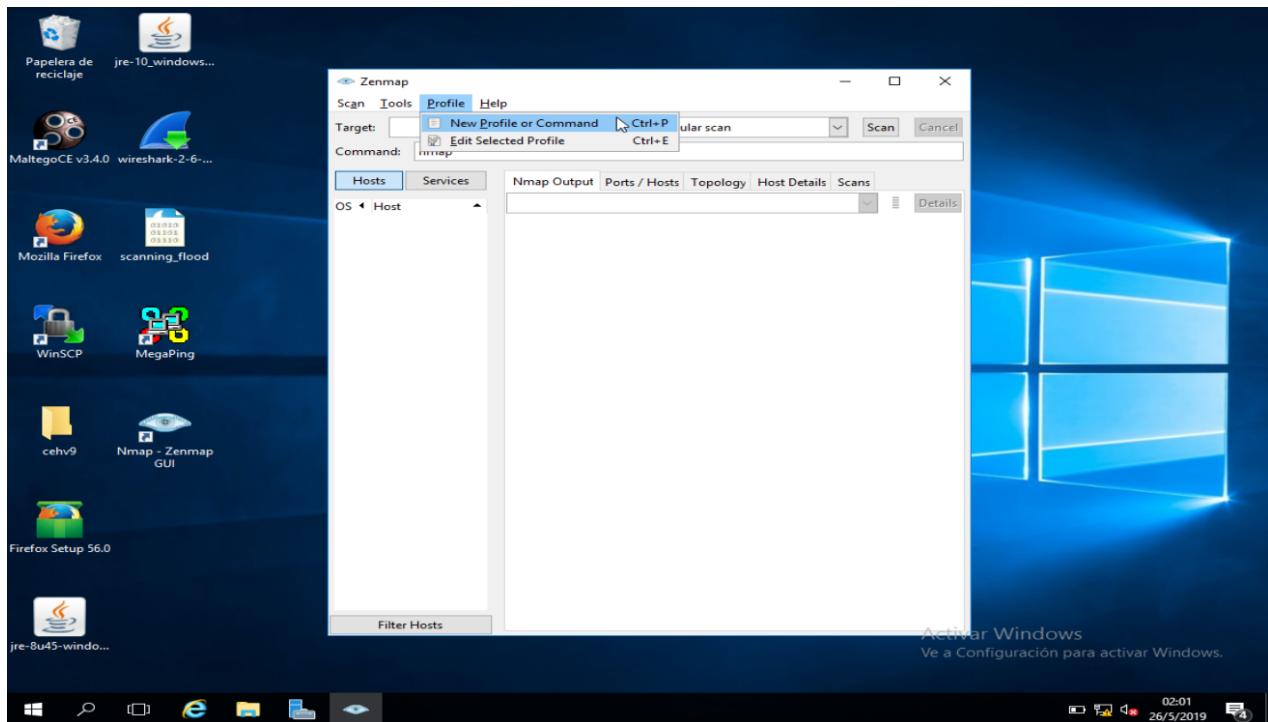


51. La exploración nula envía un paquete sin el indicador activado. Solo funciona si la implementación de TCP / IP del sistema operativo se desarrolla de acuerdo con RFC 793. En una exploración nula, los atacantes envían una trama TCP a un host remoto sin indicadores.

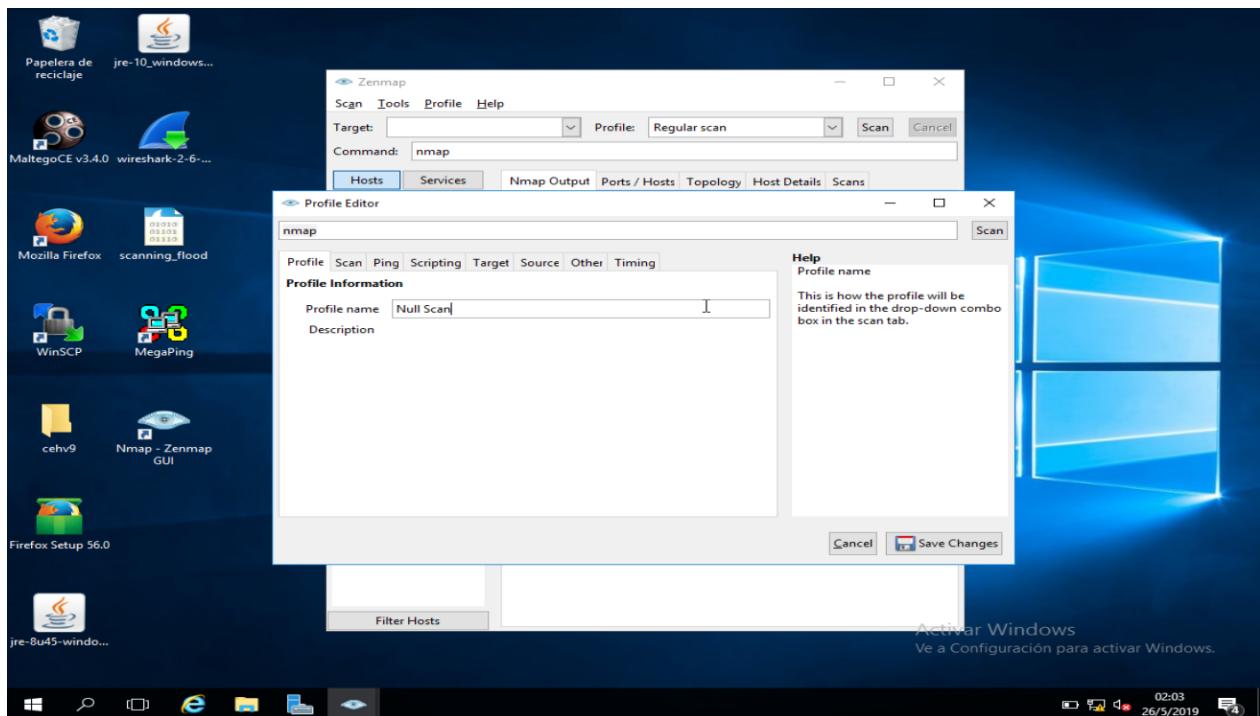
52. En el campo **Perfil**: seleccione **Escaneado regular** en la lista desplegable.



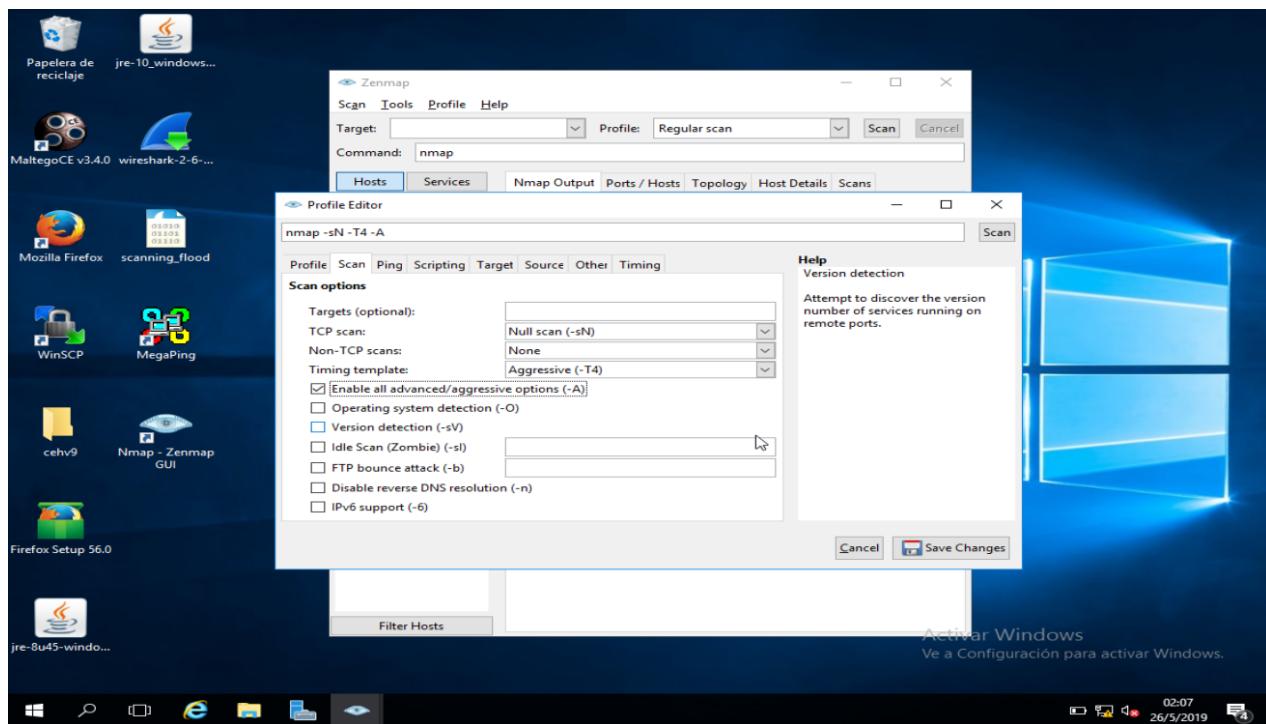
53. Para realizar un análisis nulo de una dirección IP de destino, debe crear un nuevo perfil. Haga clic en **Perfil -> Nuevo perfil or command**.



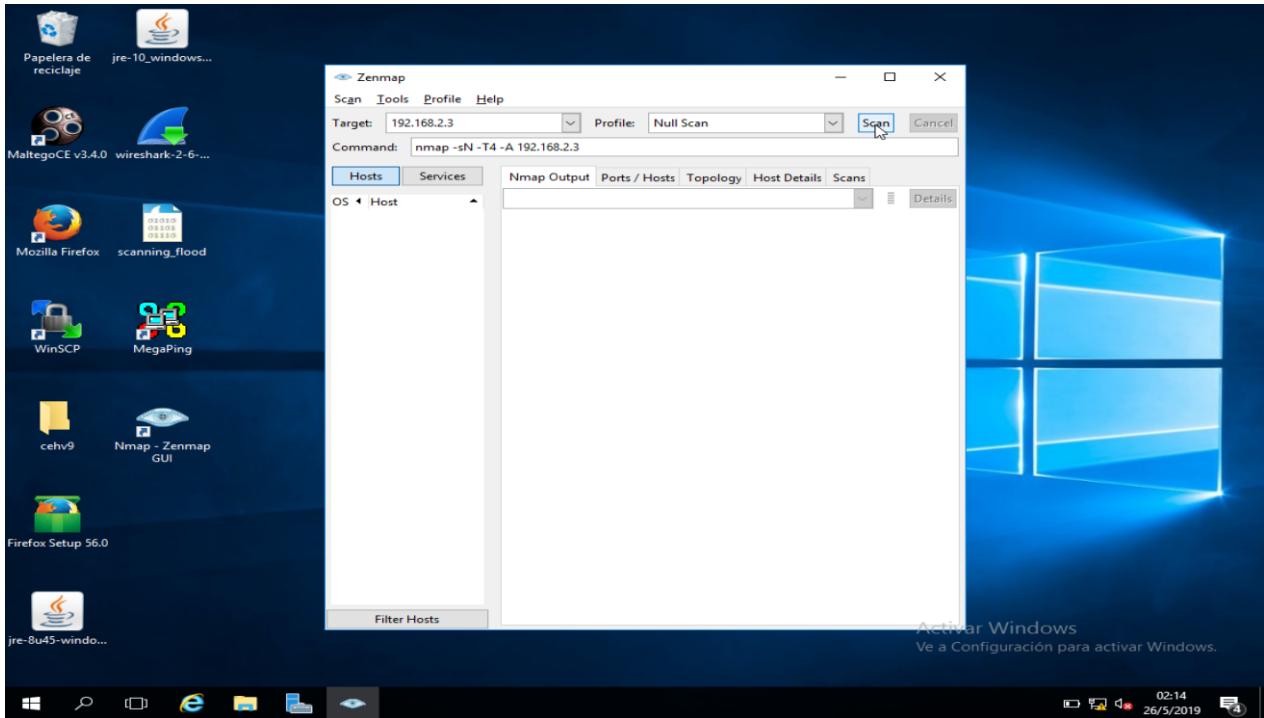
54. En la pestaña **Perfil**, ingrese un nombre de perfil **Null Scan** en el campo Nombre de perfil.



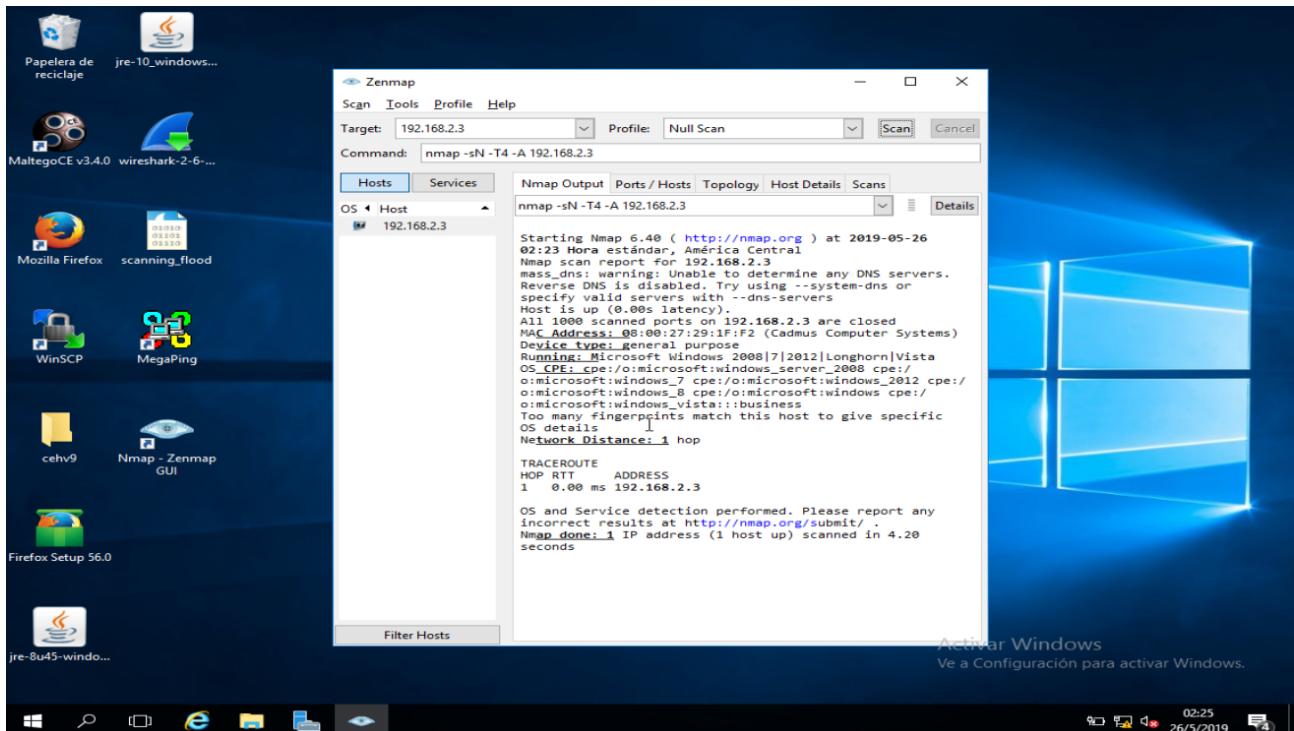
55. Haga clic en la pestaña **Escanear** en la ventana **Editor de perfiles**. Seleccione la opción **Exploración nula** (-sN) en la lista desplegable de **exploración TCP**:
56. Seleccione **Ninguno** en la lista desplegable **Exploraciones no TCP**: y **Agresivo** (-T4) en la lista **Plantilla de tiempo**: Marque la opción **Habilitar todas las opciones avanzadas / agresivas** (-A) y haga clic en **Guardar cambios**.
57. Con esta configuración, está configurando Nmap para realizar un escaneo nulo con la plantilla de tiempo como -T4 y todas las opciones agresivas habilitadas.



58. En la ventana principal de Zenmap, ingrese la **dirección IP de destino** (aquí, **192.168.2.3** que pertenece a la máquina virtual de **windows 7**) para escanear, seleccione el perfil de **escaneo nulo** en la lista desplegable **Perfil** y luego haga clic en **Escanear**.



59. Al emitir el comando, Nmap envía paquetes TCP sin ninguno de los indicadores TCP establecidos en el paquete. Si la exploración devuelve un paquete RST, significa que el puerto está cerrado; sin embargo, si no se devuelve nada, el puerto está filtrado o abierto.
60. Nmap escanea el objetivo y muestra los resultados en la pestaña Salida de Nmap.



61. Puede hacer clic en las otras pestañas para examinar los resultados obtenidos por Nmap.

