Recopilando información de código abierto usando utilidades de la interfaz de línea de comandos de Windows

Windows provee poderosa utilidades en su línea de comandos que ayudan a un hacker ético a reunir información acerca de un objetivo de evaluación.

El objetivo de este laboratorio es mostrar cómo usar ping, nslookup y traceroute para reunir información acerca de un objetivo:

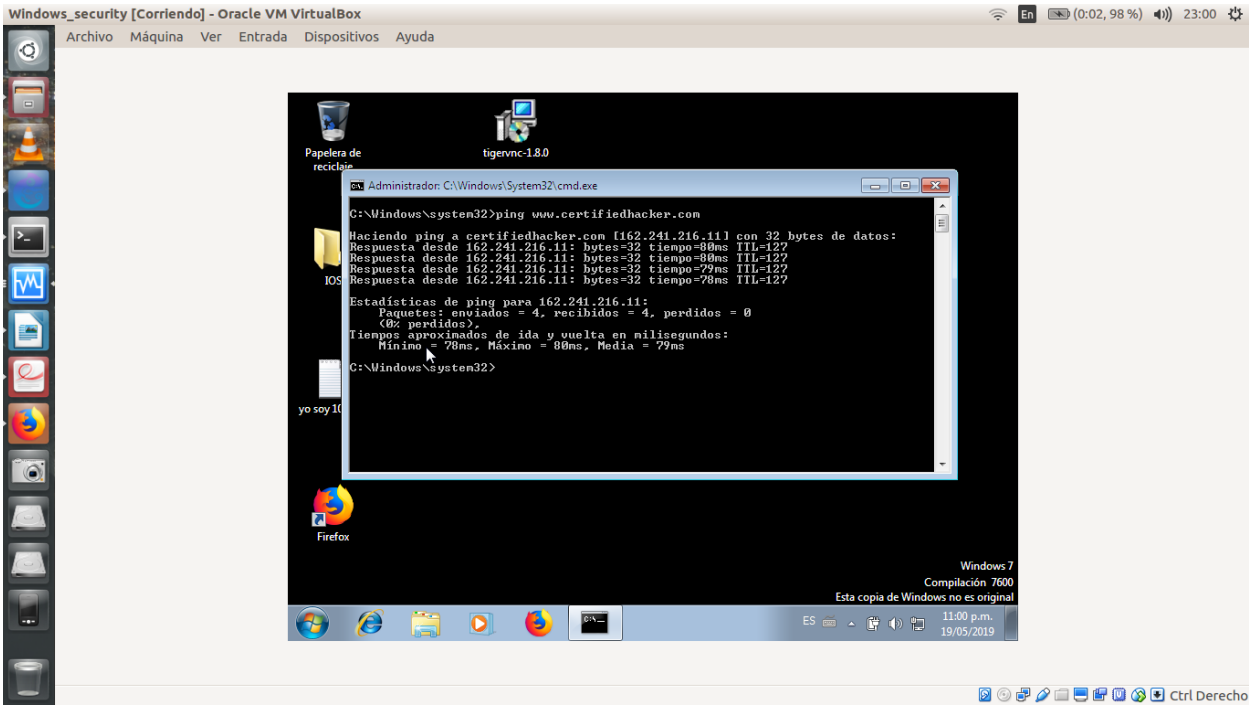
- Usar la utilidad **ping** para encontrar la IP del dominio del objetivo
- Utilizar **ping** para emular el comando tracert (traceroute)
- Encontrar el tamaño máximo de trama para la red
- Identificar el tipo de **ICMP** y código para una respuesta de echo y paquetes de respuesta.

Tareas de laboratorio:

1. Encontrar la dirección IP para www.certifiedhacker.com

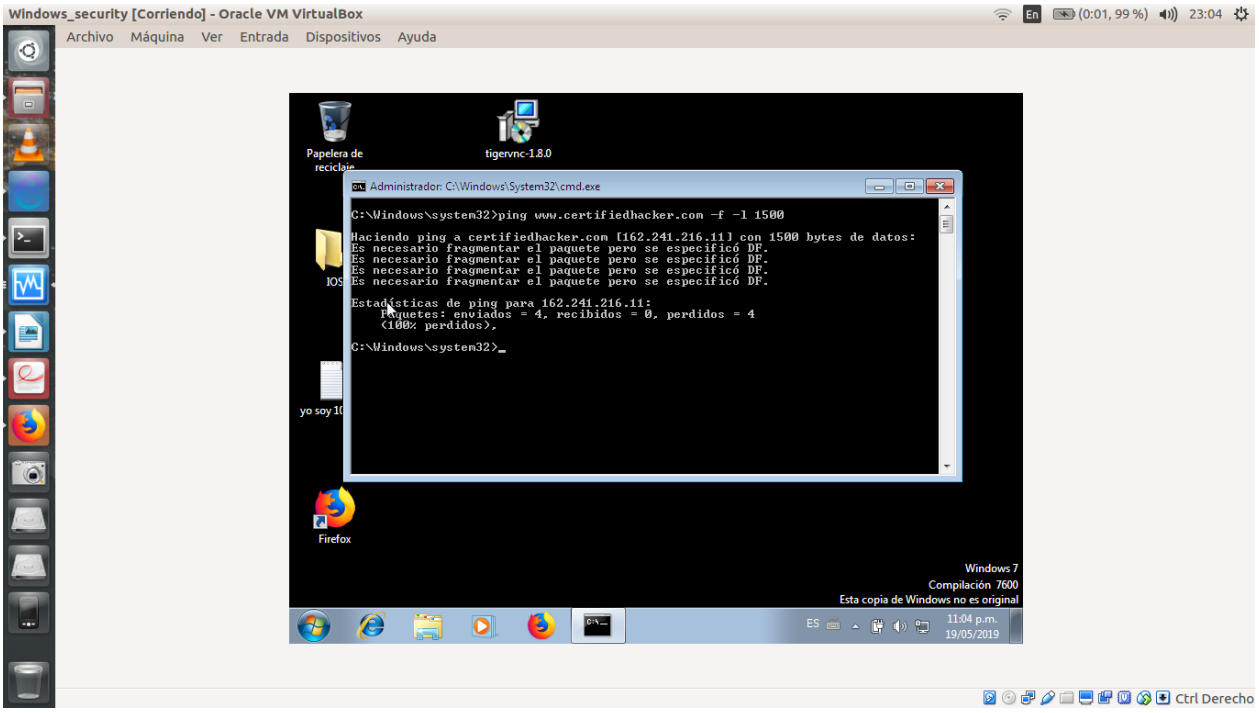
2. Para hacer esto se debe dirigir a la línea de comandos de Windows

3. Ahora se deberá escribir **ping www.certifiedhacker.com** en la línea de comandos y presionar **Enter** para encontrar su dirección IP. Esta respuesta deberá ser similar a la de la siguiente captura



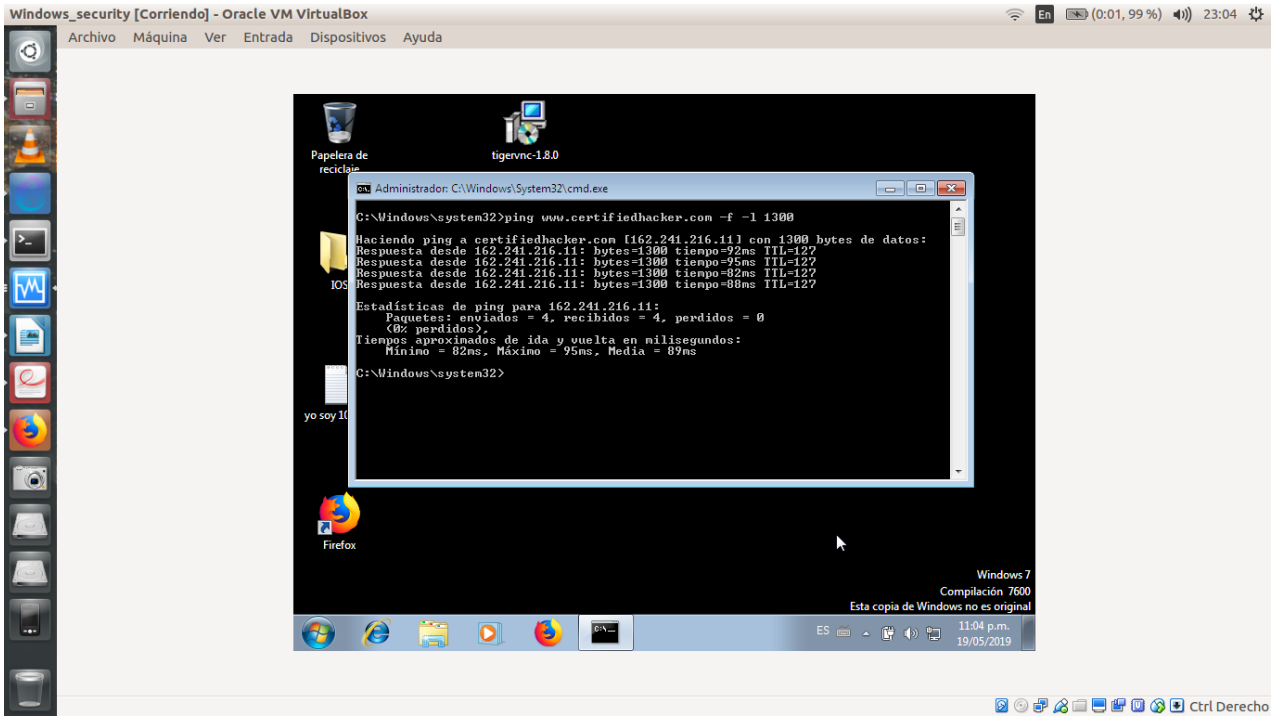
4. Note que la dirección IP del objetivo es 162.241.216.11, además puedes obtener información acerca de las estadísticas del Ping tales como los paquetes enviados, los paquetes perdidos.

5. Ahora vamos a encontrar el tamaño máximo de la trama en la red, para ello vamos a escribir en la línea de comando de Windows el siguiente comando **ping www.certifiedhacker.com –f –l 1500**



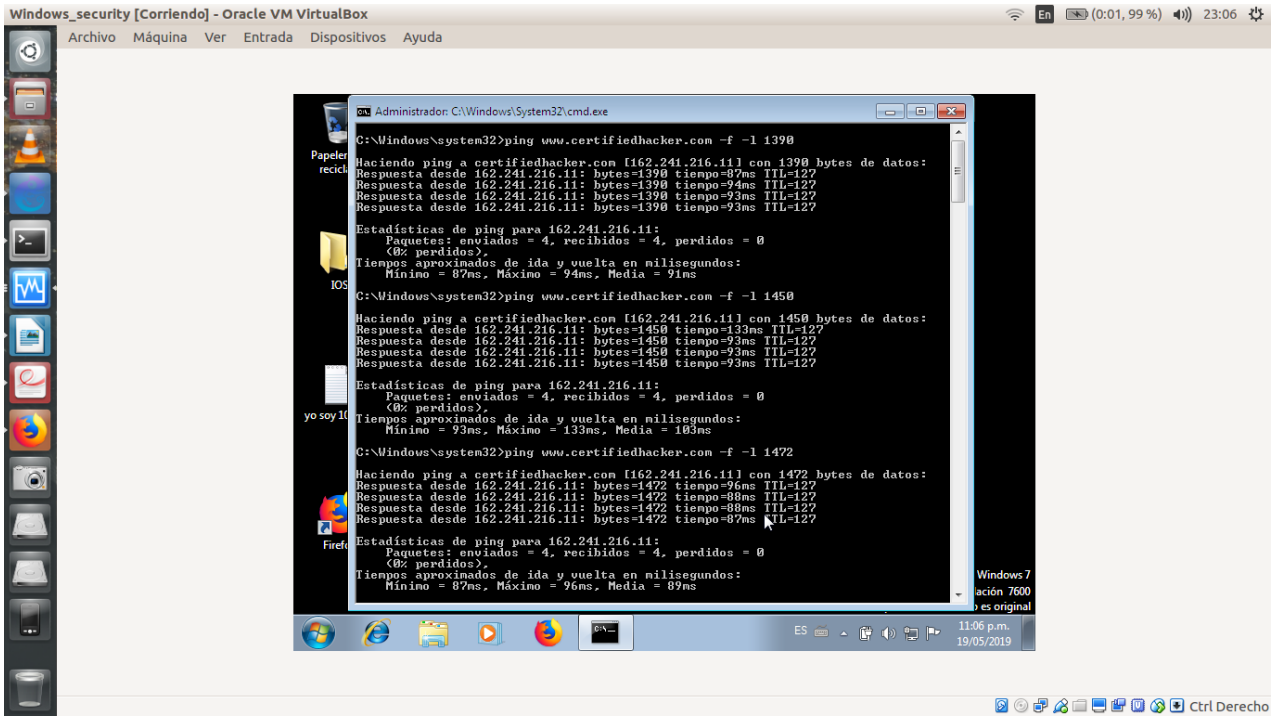
6. La respuesta devuelta debe de ser **Packet needs to be fragmented but DF set** significa que la trama es muy grande para ser enviada por la red y necesita ser fragmentada. Ya que usamos el parámetro –f con el comando ping, el paquete no ha sido enviado y el comando ping ha retornado un error.

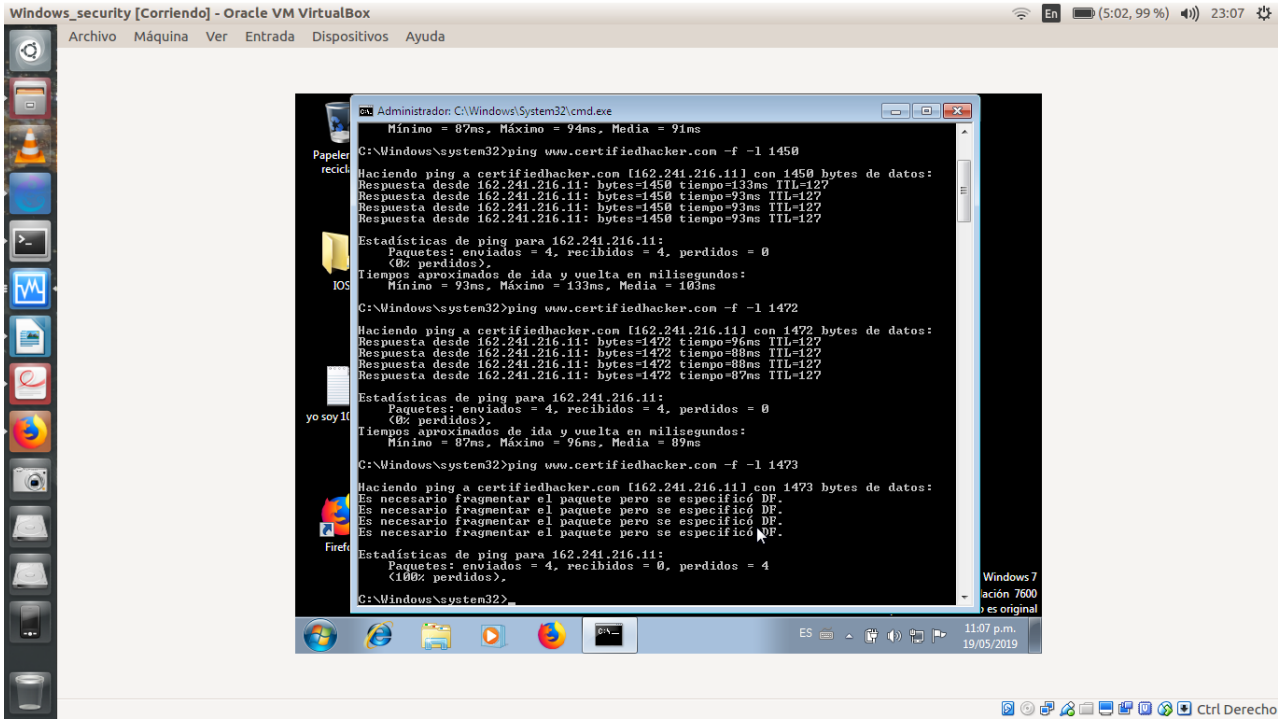
7. Vamos a escribir ahora **ping www.certifiedhacker.com –f –l 1300**



8. Observamos que el tamaño máximo de paquetes es menos que 1500 y más que 1300 bytes.

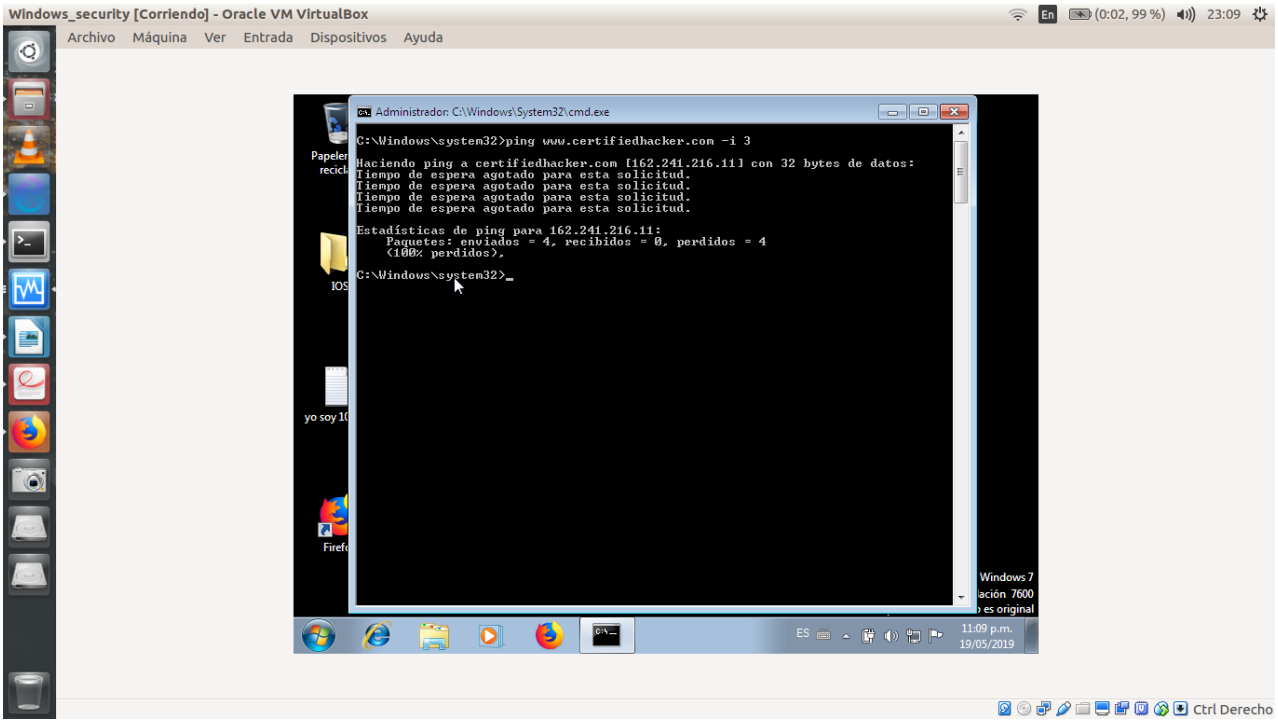
9. Ahora trataremos diferentes valores hasta encontrar el tamaño máximo de la trama en la red para eso usaremos el comando anterior **ping www.certifiedhacker.com –f –l 1300** e iremos aumentando el tamaño de la trama hasta llegar a su valor máximo





10. Lo siguiente seria descubrir cuando el tiempo de vida llega expirar, cada paquete sobre la red tiene un tiempo de vida establecido. Si el tiempo de vida es de 0 el router descarta el paquete. Este mecanismo evita la perdida de paquetes.

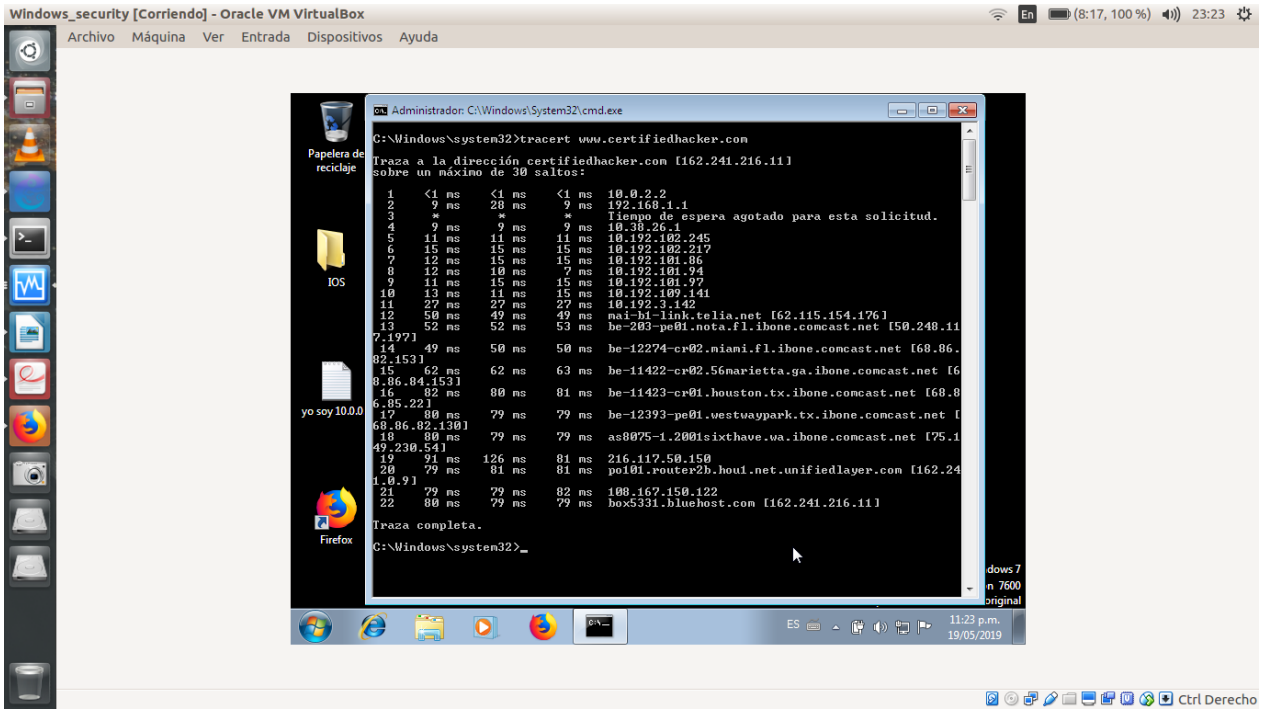
11. En la línea de comandos escribiremos **ping www.certifiedhacker.com –i 3** esto establece el tiempo de vida con un valor de 3.



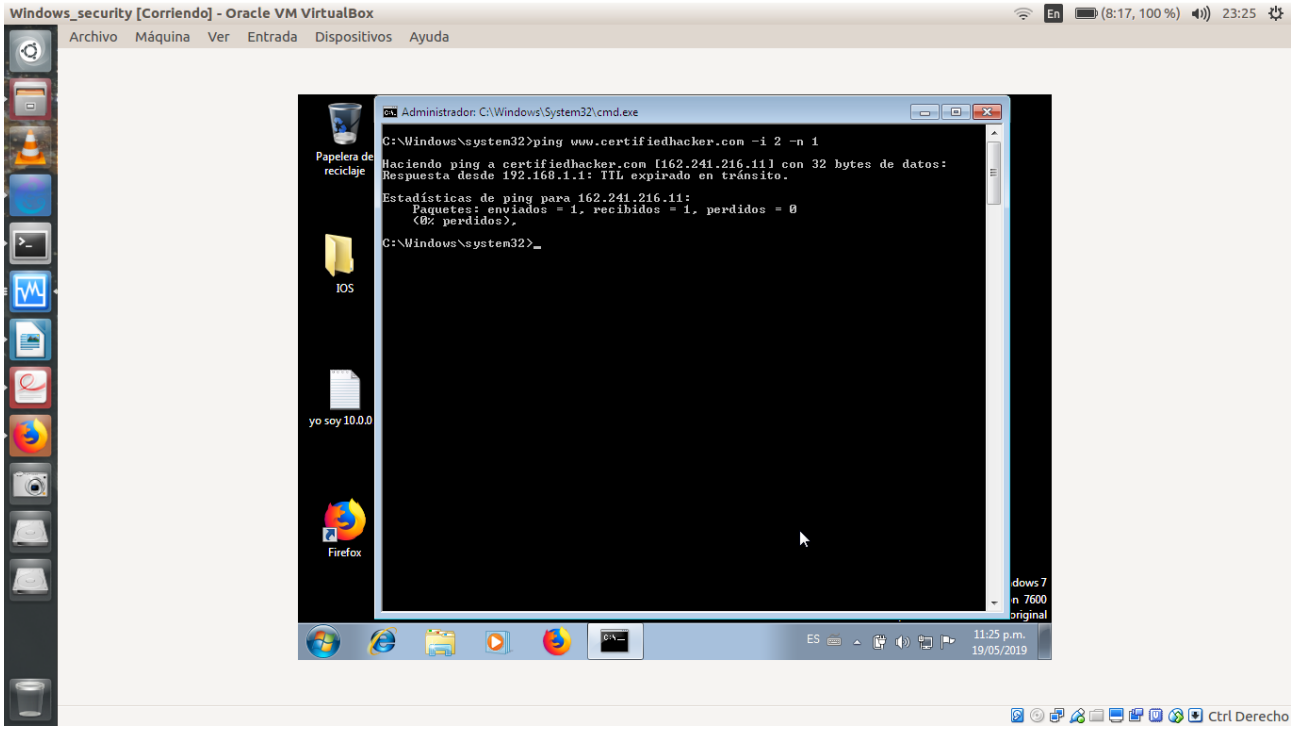
12. Como podemos observar en la imagen anterior el paquete ha sido descartado por los routers intermedios ya que su tiempo de vida era menor que el número de saltos que este da para llegar a su destino.

13. De esta manera nosotros podemos usar el comando ping para emular un traceroute.

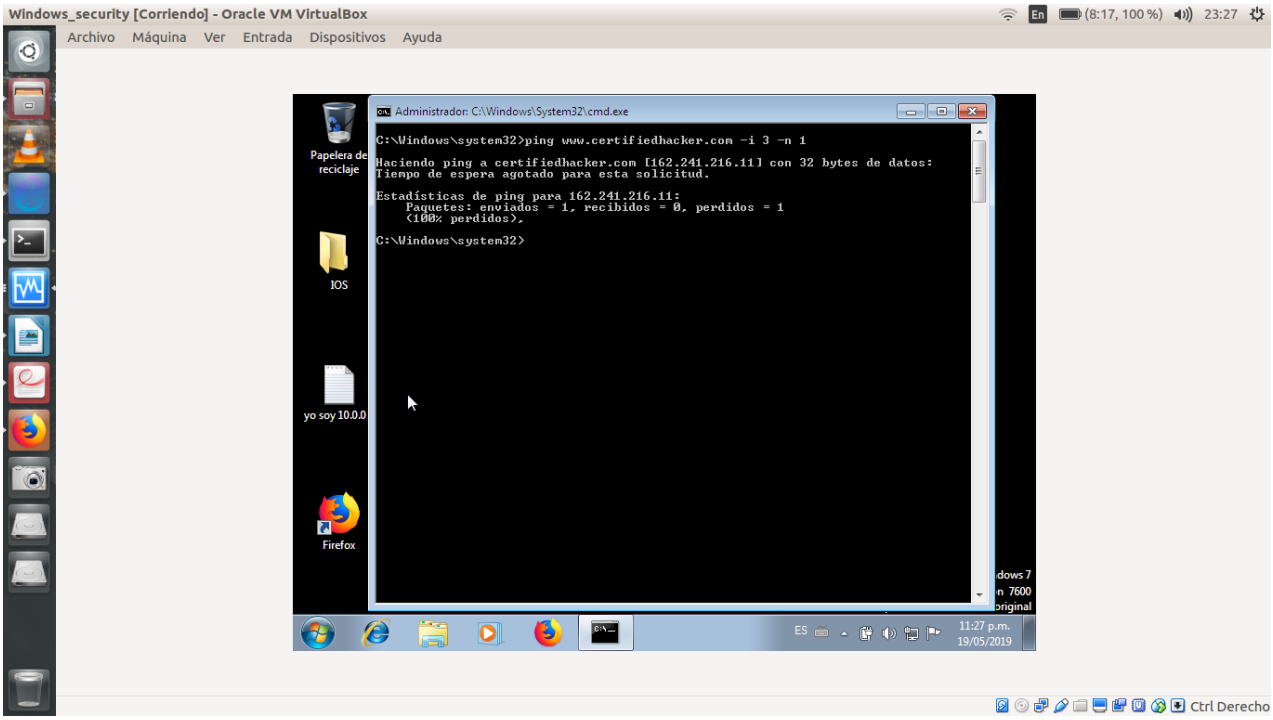
14.Lanzaremos una nueva línea de comandos y escribiremos **tracert www.certifiedhacker.com** este comando rastreara la información de configuración de red del dominio del destino.



15. Minimizaremos la línea de comandos mostrada anteriormente y lanzaremos una nueva. En esta escribiremos **ping www.certifiedhacker.com –i 2 –n 1**. La única diferencia con el comando anterior es que ahora establecemos el tiempo de vida con un valor de 2 intentando verificar el tiempo de vida de los paquetes.

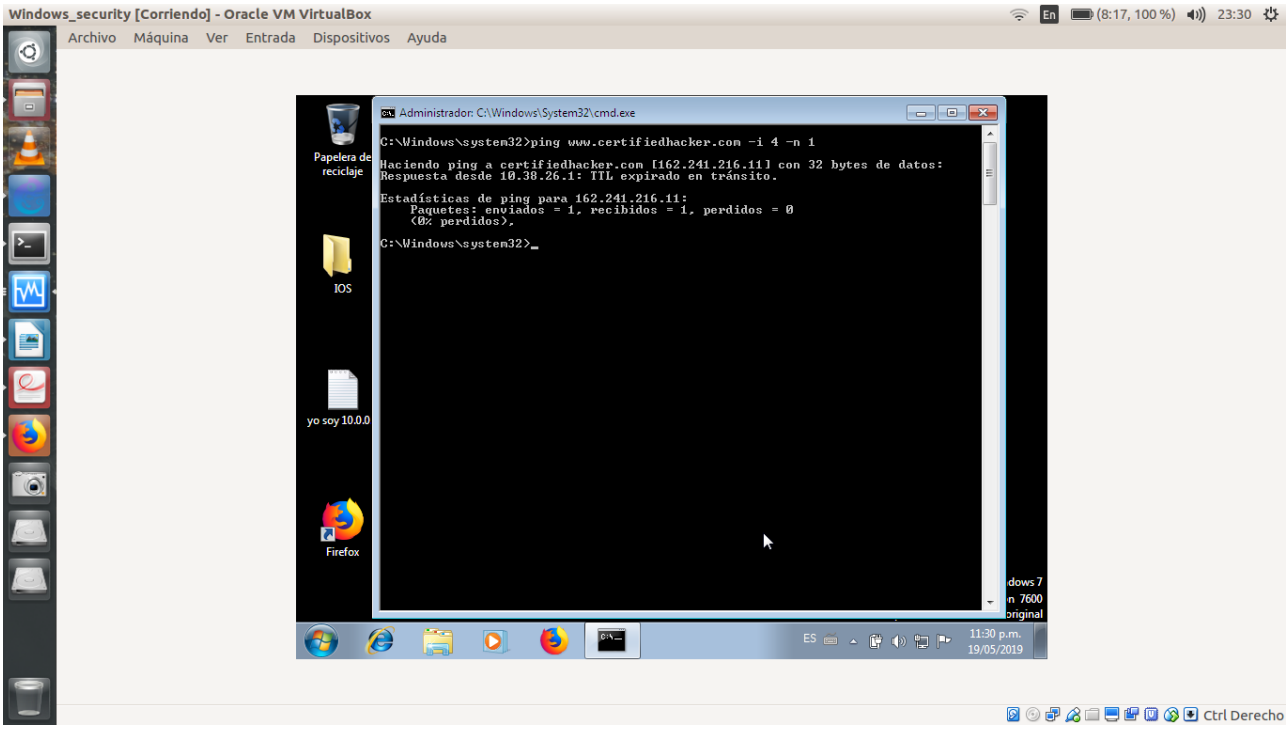


16. Ahora escribiremos **ping www.certfiedhacker.com –i 3 –n 1**



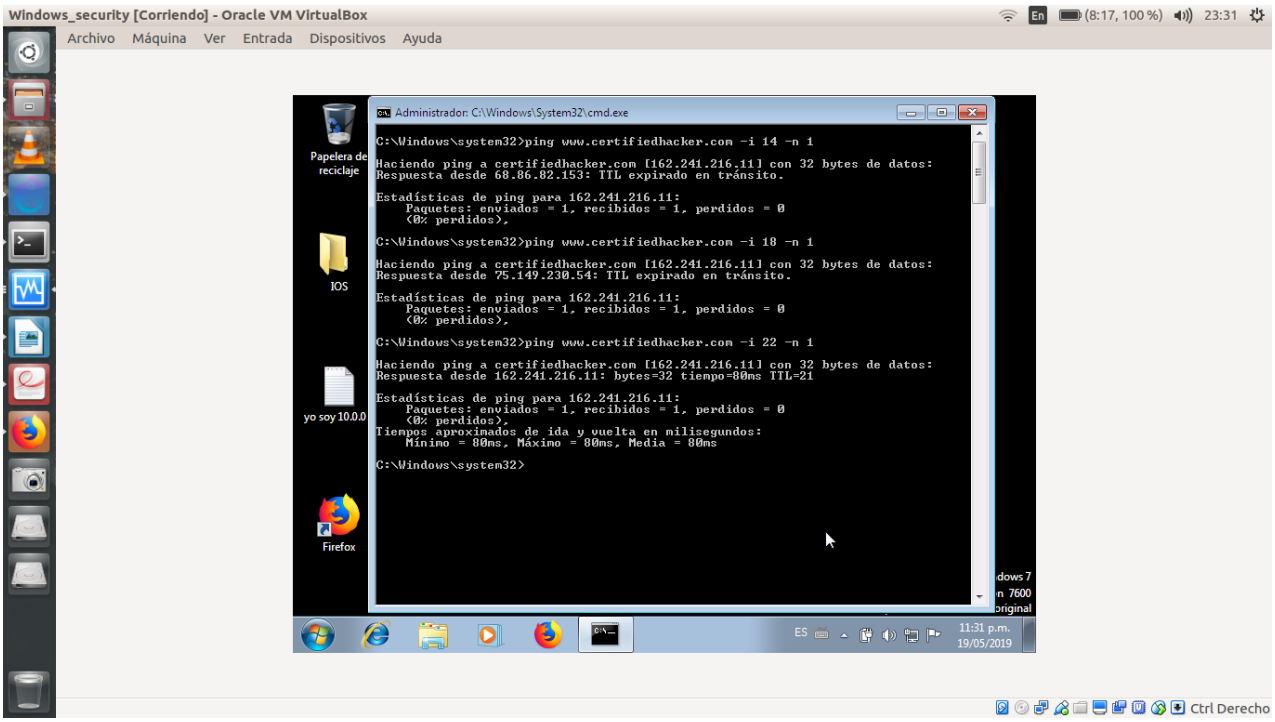
17. Observamos que no hay una respuesta

18. Aplicaremos la misma sintaxis del apartado anterior pero esta vez estableceremos el tiempo de vida con un valor de 4.



19. Repita el paso anterior hasta que puedas alcanzar la IP asociada al dominio **www.certifiedhacker.com**.

20. El resultado de todo este trabajo es mostrado en la siguiente imagen

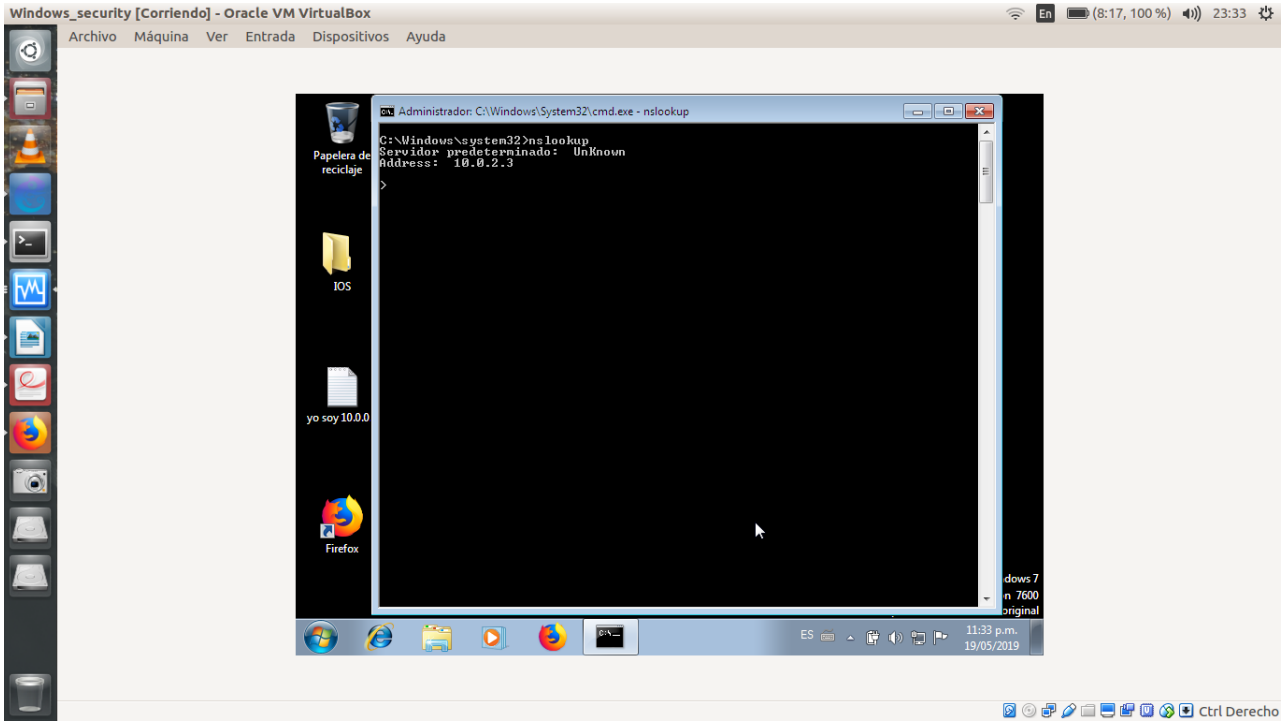


21. Esto implica que al establecer el tiempo de vida con un valor de 22 recibimos respuesta por parte del destinatario host.

22. Las direcciones IP reflejadas en la imagen anterior son:

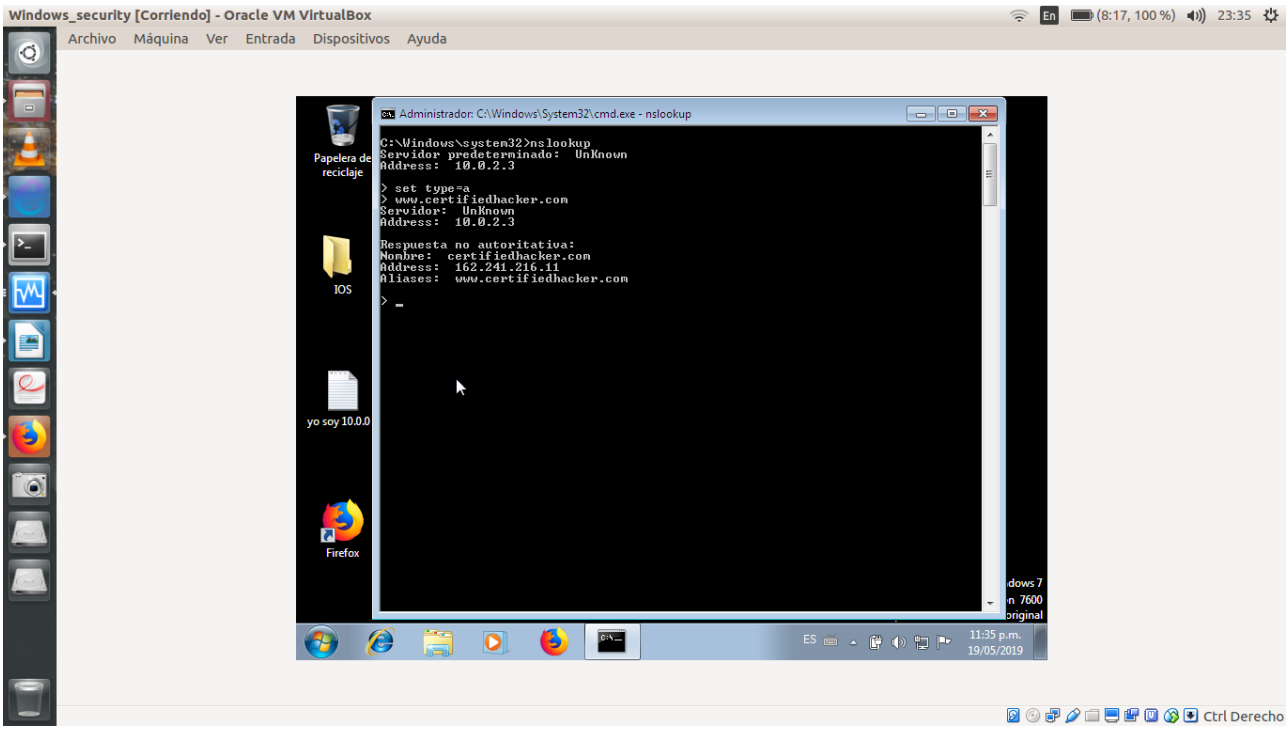
- 68.86.82.153
- 75.149.230.54

23. Vamos a lanzar una nueva línea de comandos y escribiremos **nslookup**. Esto nos mostrara el servidor por defecto la dirección IP de nuestro servidor de nombres.



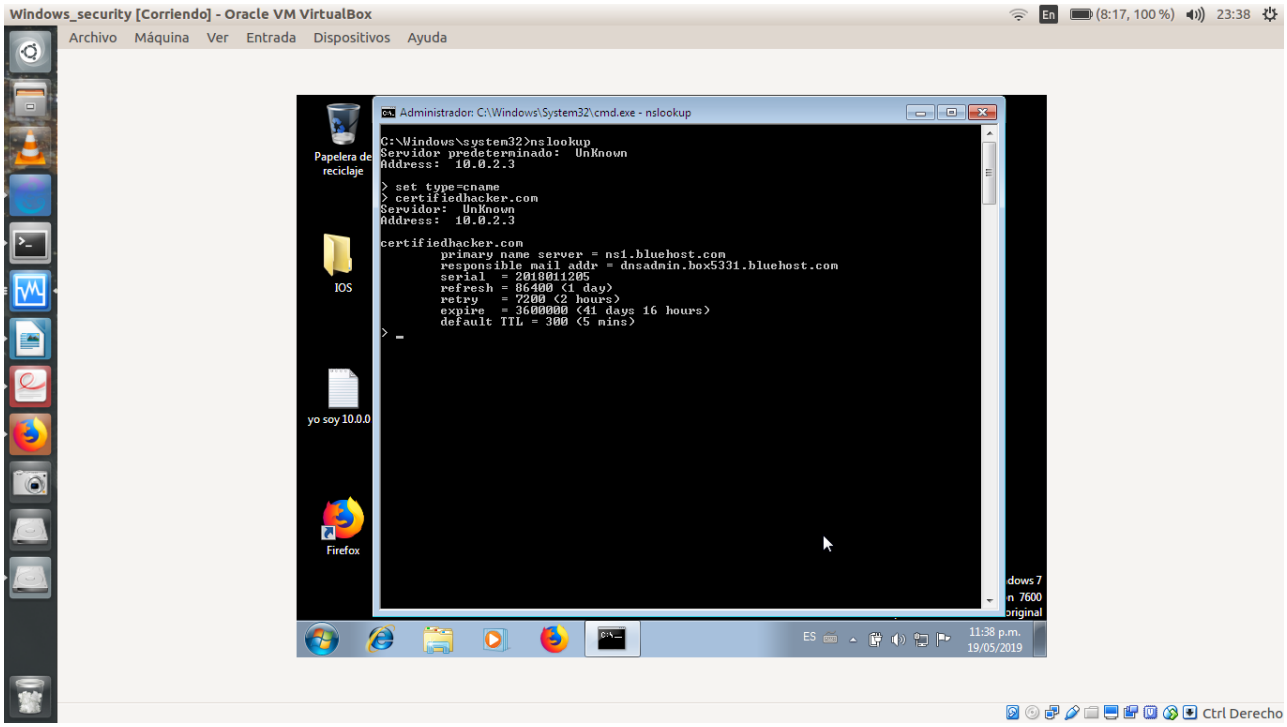
24. En el modo interactivo de nslookup, escribiremos set type=a y presionaremos Enter. Esta configuración consulta la dirección IP del dominio dado.

25. Escribimos **certifiedhacker.com** y presionamos **Enter**. Esto resolverá la dirección IP y mostrará los resultados en pantalla



26. Ya que la respuesta es no autoritativa, nosotros necesitaremos obtener el nombre de dominio autoritativo del servidor.

27. Vamos a escribir **set type=cname** y presionar **Enter**. la búsqueda cname se hace directamente contra el nombre de dominio autoritativo del servidor y lista los registros cname para un dominio.

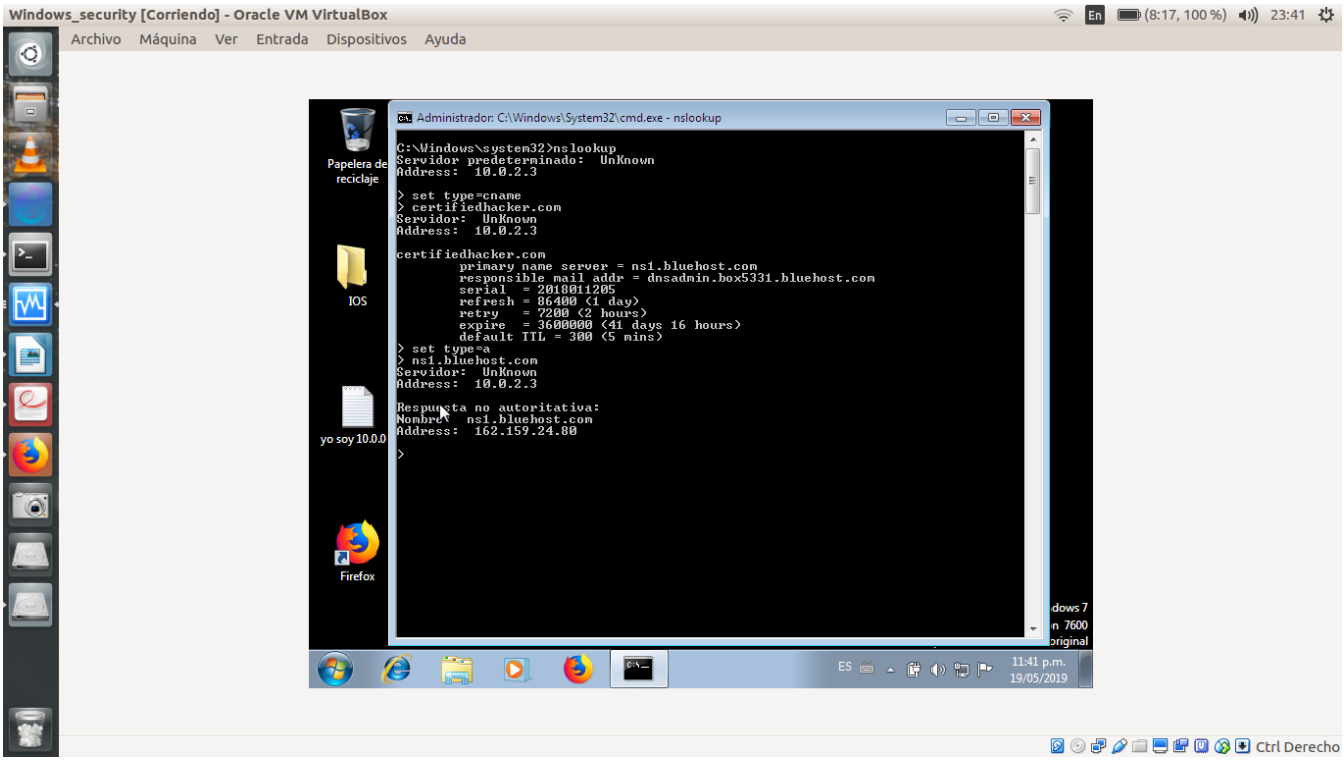


28. El resultado obtenido es el nombre del servidor autoritativo a lo largo con el email del servidor

29. Ahora que tenemos el nombre del servidor autoritativo necesitaremos determinar la dirección IP del servidor de nombres.

30. Para ello volveremos a establecer el valor de **set type=a** y presionar **Enter**.

31. Escribiremos en la línea de comandos ns1.bluehost.com y presionamos Enter. Esto devolverá la dirección del servidor como se muestra en la siguiente imagen.



el servidor de nombre autoritario almacena los registros asociados con el dominio. por lo tanto, si un atacante puede determinar el servidor de nombres autoritativo y obtener su dirección IP asociada, puede intentar explotar el servidor para ejecutar los ataques como DOS, DDOS, re direccionamiento URL entre otros.