Lab

11

Realización de enumeración de red utilizando varias herramientas de interrogación de DNS

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a comprender y antes de varias técnicas de enumeración para:

- Extraer información de Whois

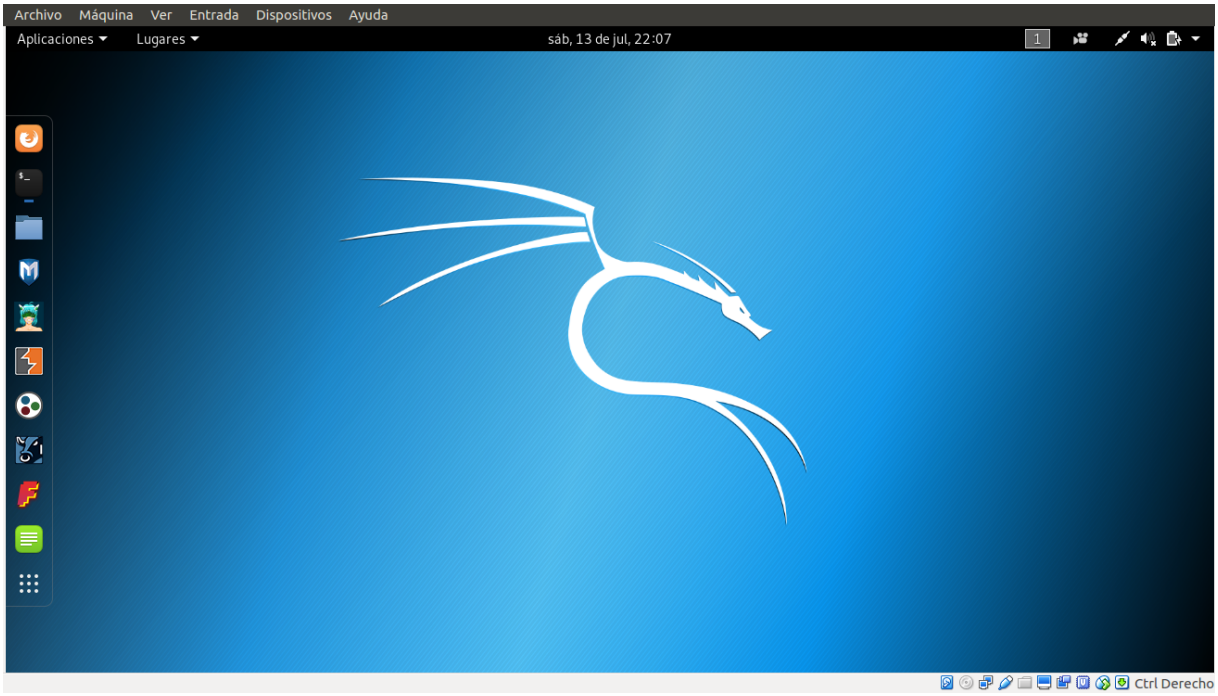
Visión general de enumeracion

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, redes, recursos, recursos compartidos y servicios de un sistema. Las técnicas de enumeración se realizan en un entorno de intranet.

Tareas del laboratorio

1. Inicie la máquina virtual Kali Linux desde el Administrador de Hyper-V e inicie sesión en ella.

2. Aparece el escritorio de la máquina Kali Linux, como se muestra en la siguiente captura de pantalla.



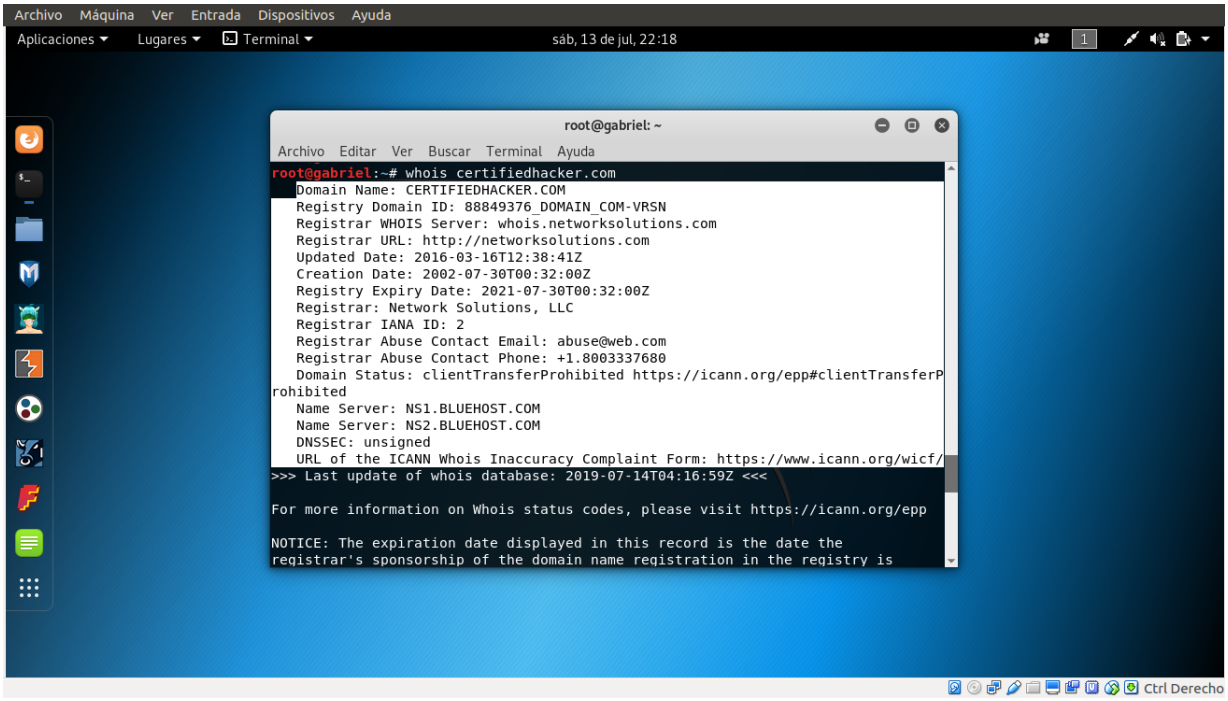
3. Seleccione **Aplicaciones -> Accessories → Terminal** esto nos lanzara una linea de comandos.

4. Alternativamente, puede hacer clic en el icono de Terminal de línea de comando, ubicado en la barra de tareas.

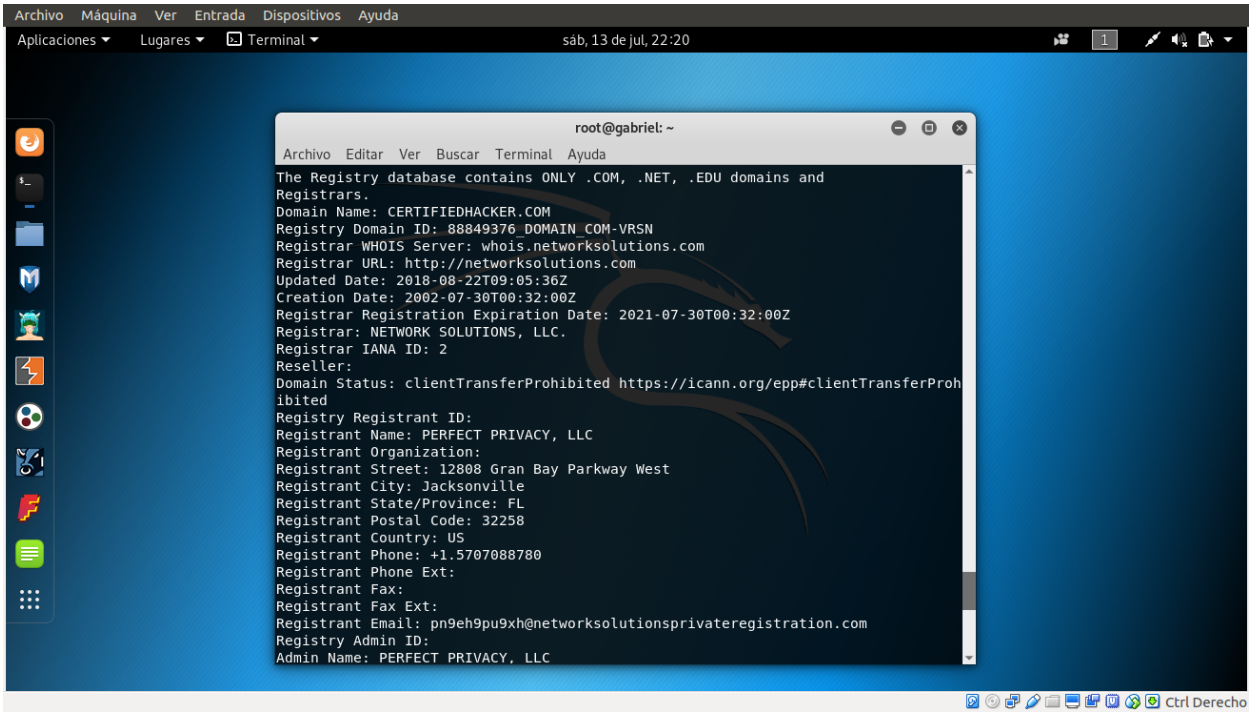
5. El objetivo utilizado en este laboratorio es www.certifiedhacker.com; su nombre de dominio correspondiente es certifiedhacker.com.

6. Escriba **whois certifiedhacker.com** en la línea de comando y presione Enter.

7. Esto de vuelve información relacionada con whois del dominio certifiedhacker.com

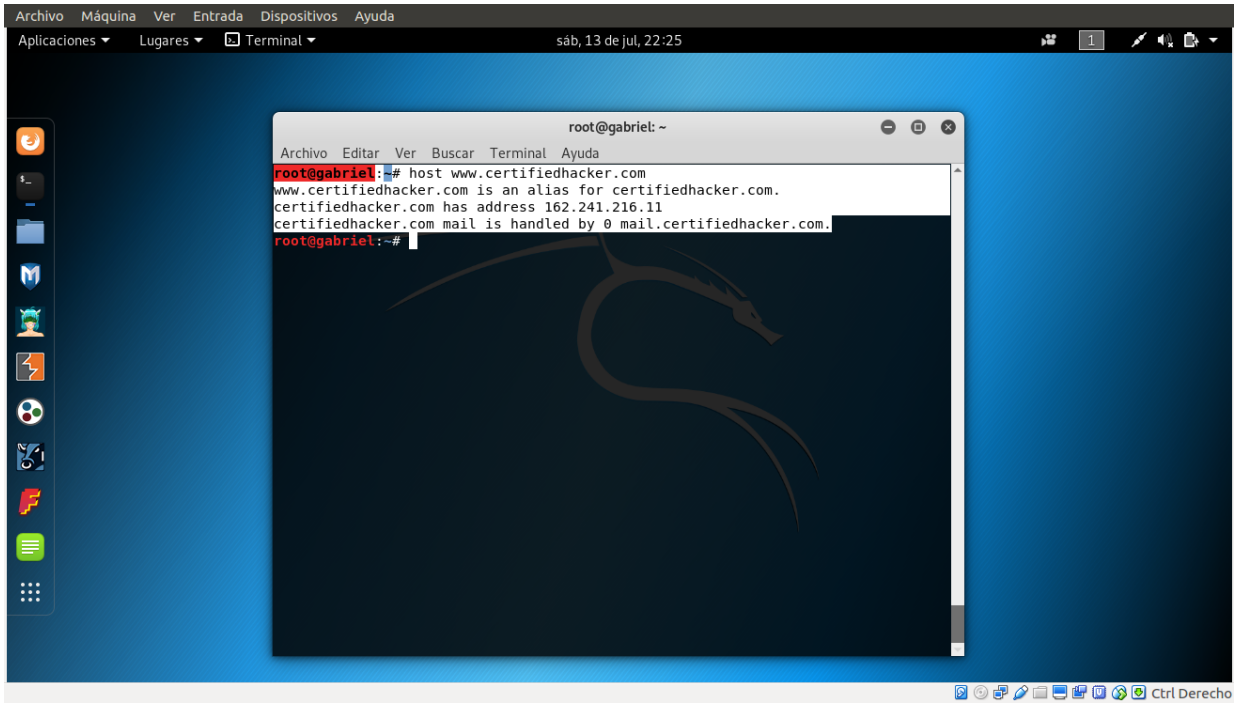


8. Desplácese hacia abajo en la ventana del terminal la información relacionada con el **registrador**.

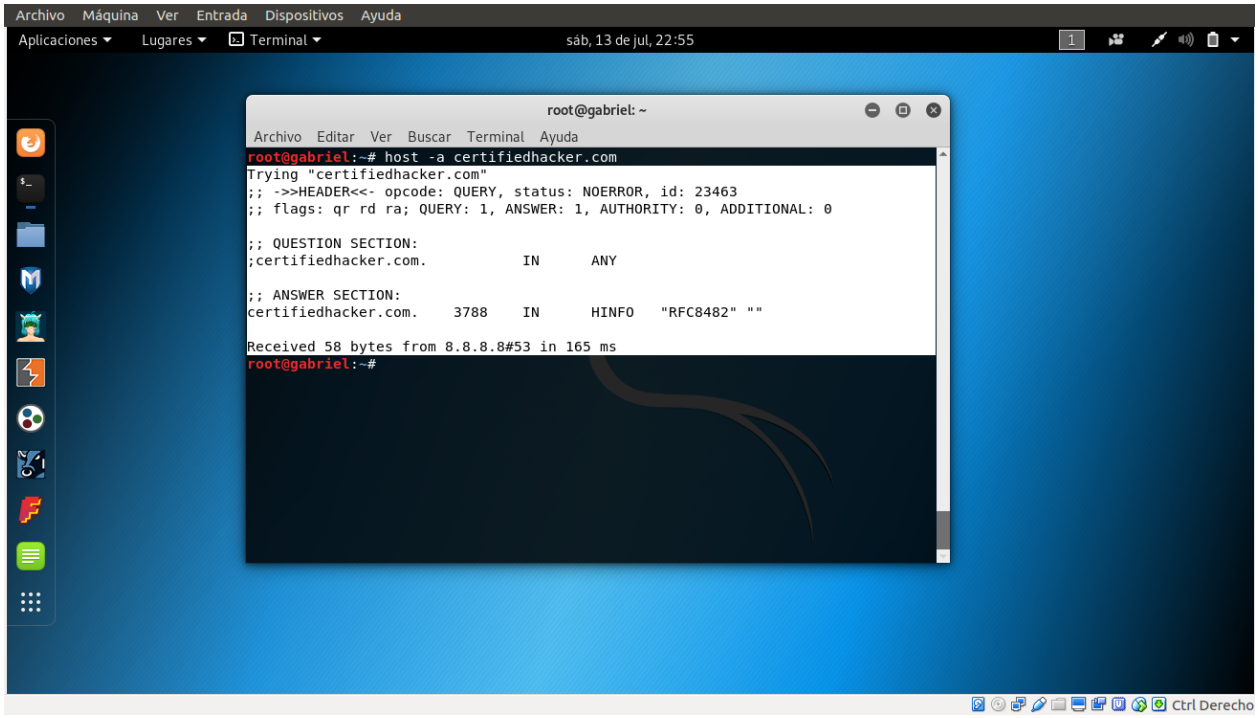


9. Escriba **host certifiedhacker.com** para enumerar la dirección IP del sitio web www.certifiedhacker.com

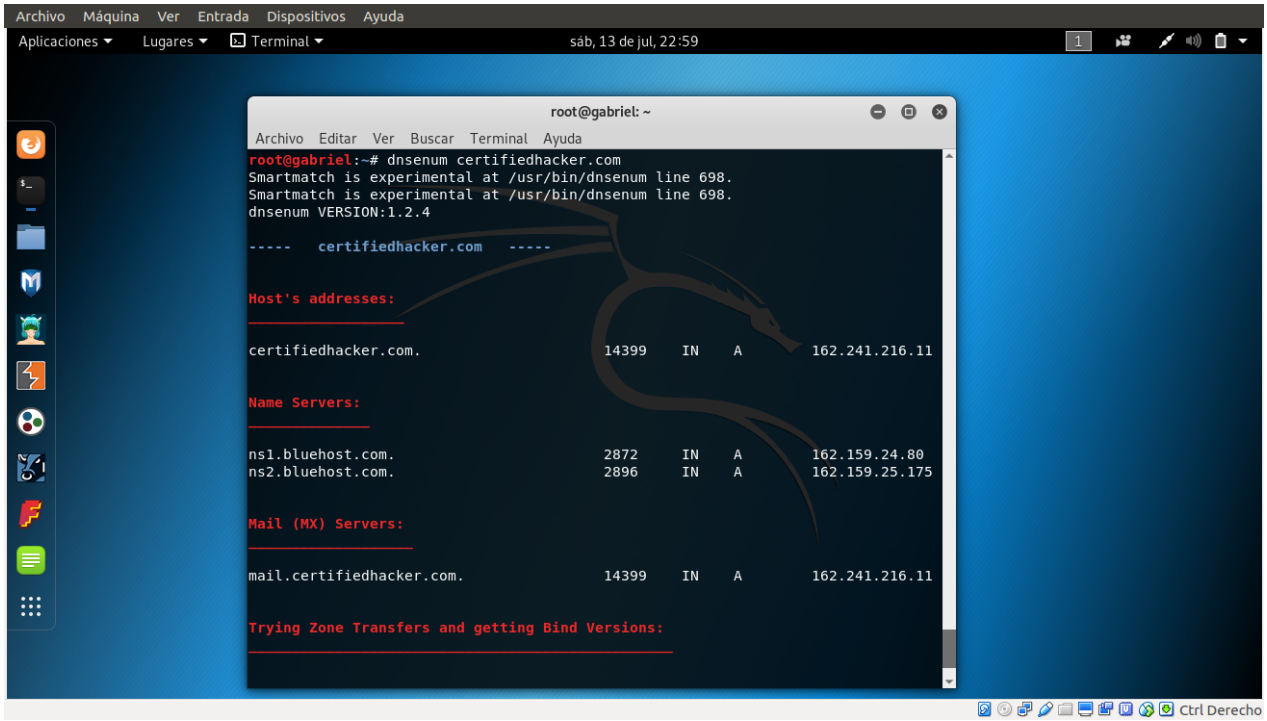
10. Se le proporcionará toda la dirección IP asociada con el sitio web de destino, como se muestra en la siguiente captura de pantalla.



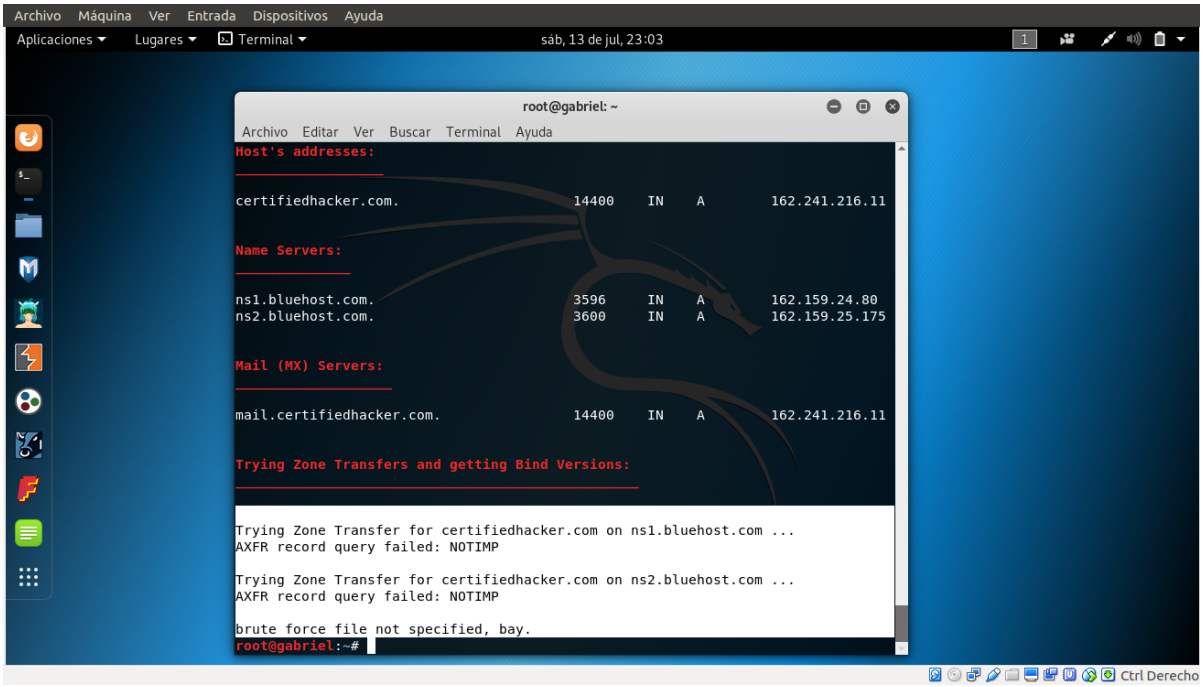
11. Escriba **host -a certifiedhacker.com** y presione **Enter** para mostrar los registros DNS asociados con el sitio web, como se muestra en la captura de pantalla.



12. Escriba **dnsenum certifiedhacker.com** y presione **Enter** para mostrar la dirección IP, los servidores de nombres, los servidores de correo y otros relacionados con el sitio web, como se muestra en la captura de pantalla.



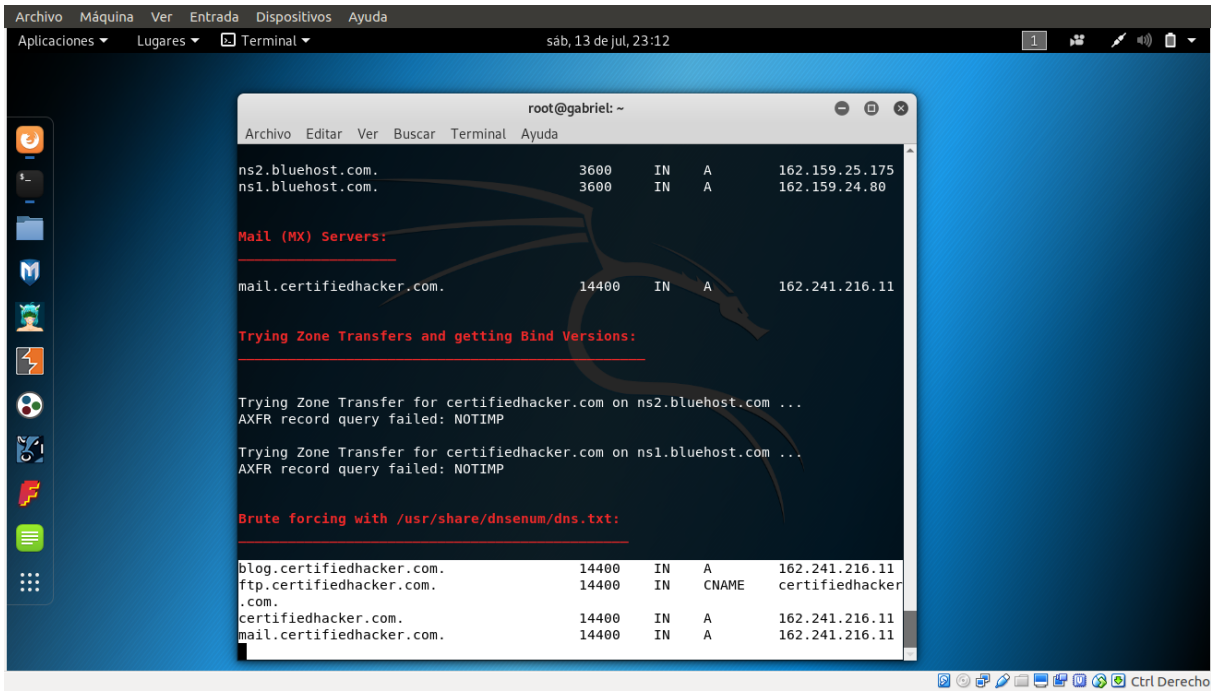
13. **dnsenum** también intenta realizar una transferencia de zona para el dominio en sus servidores de nombres asociados, en un intento de obtener subdominios, como se muestra en la captura de pantalla.

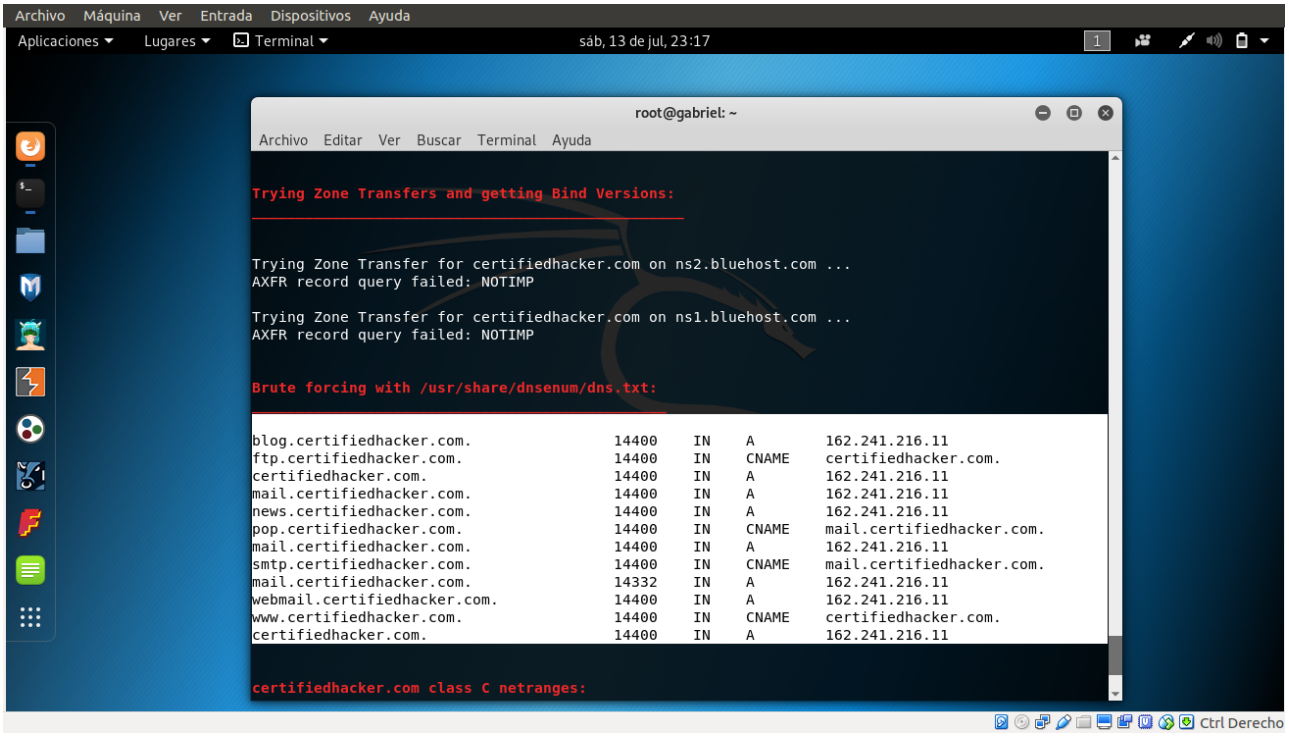


Nota: En este ejercicio no se pudo hacer la transferencia de zonas debido a que el servidor dns que alberga **certifiedhacker.com** no devuelve una respuesta.

14. En caso de que exista un archivo de transferencia de zona, puede realizar un ataque de fuerza bruta en el sitio web de destino emitiendo el comando **dnsenum -f /usr/share/dnsenum/dns.txt certifiedhacker.com** y presionando **Enter**.

15. dnsenum intenta imponer una fuerza bruta en el sitio web para extraer su subdominio, la dirección IP de clase c, etc., asociada con el sitio web.

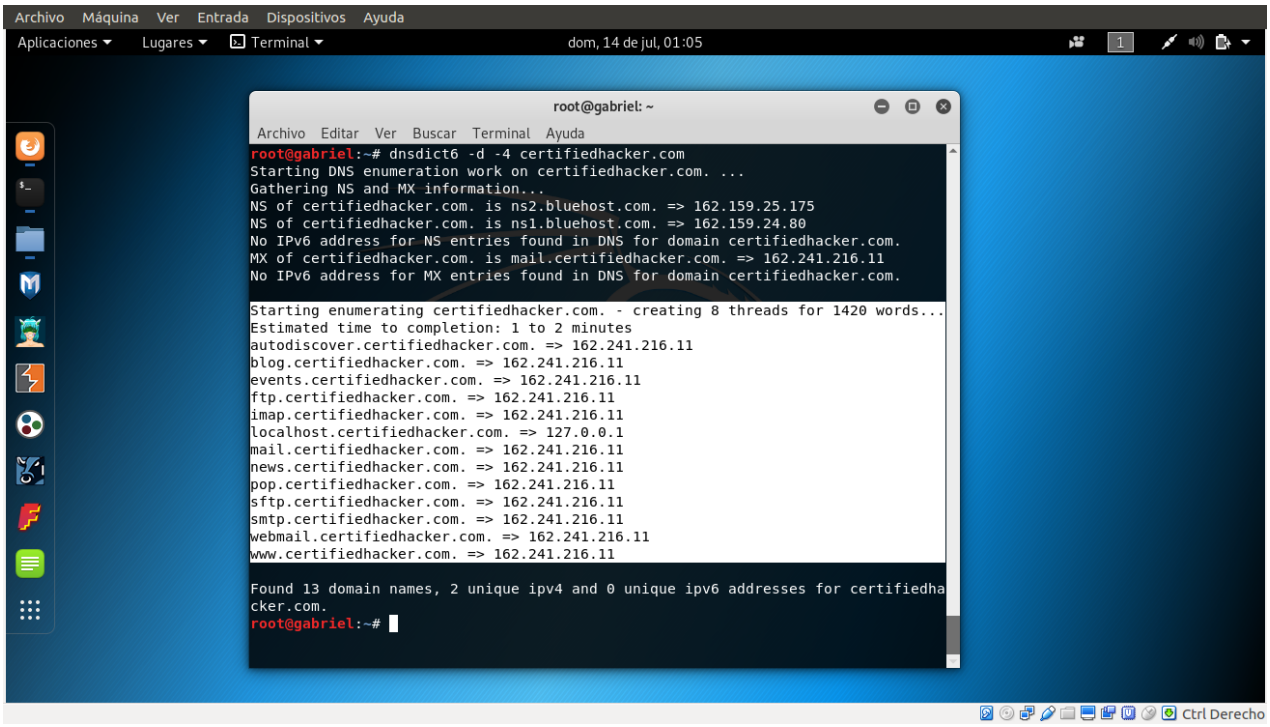




16. Escriba el comando **dnsdict6 -d -4 certifiedhacker.com** y presione **Enter**.

17. Esto:

- Enumera los subdominios en certifiedhacker.com asociados con la dirección IPv4.
- Obtiene información relacionada con DNS, como se muestra en la captura de pantalla



18. Escriba **fierce -dns certifiedhacker.com** y presione **Enter**. Esto enumera la información relacionada con el servidor de nombres, junto con los subdominios asociados con el sitio web, como se muestra en la captura de pantalla.