



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 aplicar varias técnicas de enumeración para:

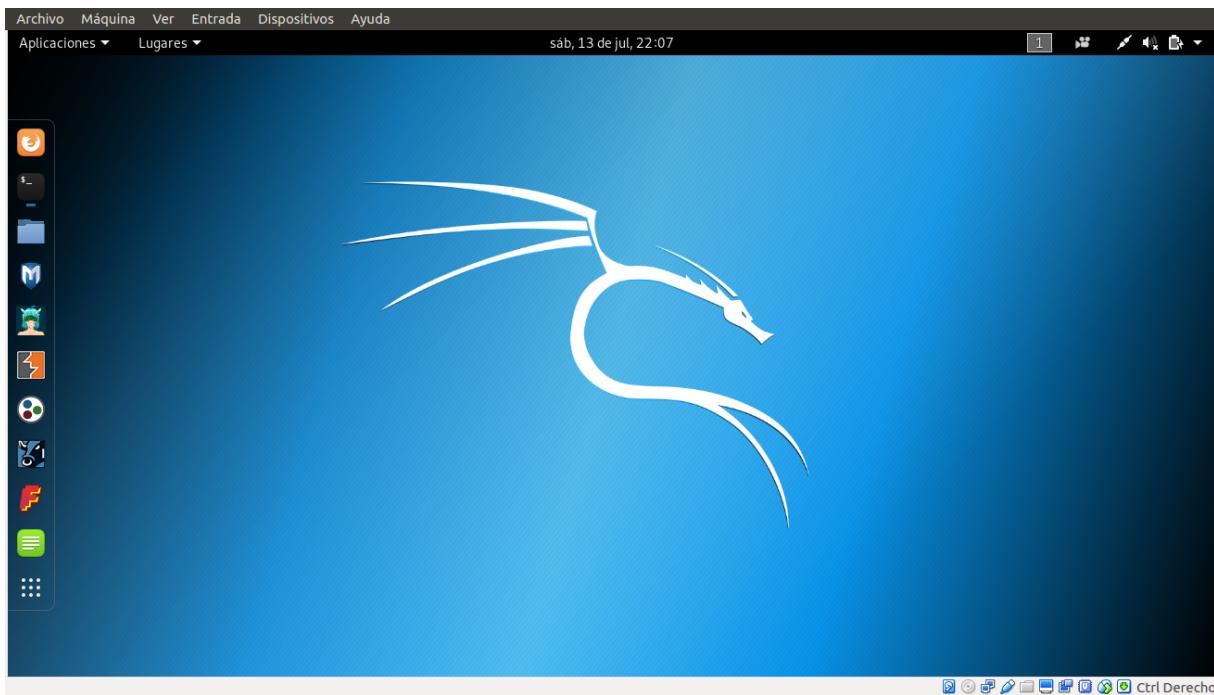
- Extraer información de Whois

Visión general de enumeración

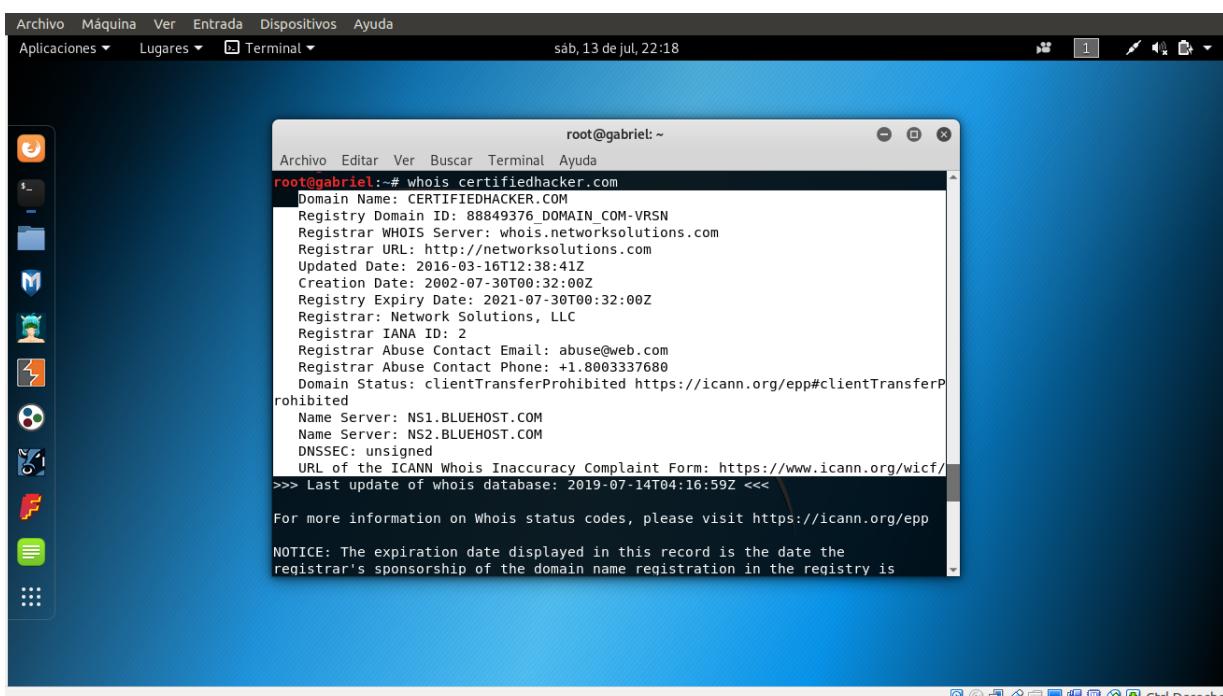
La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, redes, recursos, recursos compartidos y servicios de un sistema. Las técnicas de enumeración se realizan en un entorno de intranet.

Tareas del laboratorio

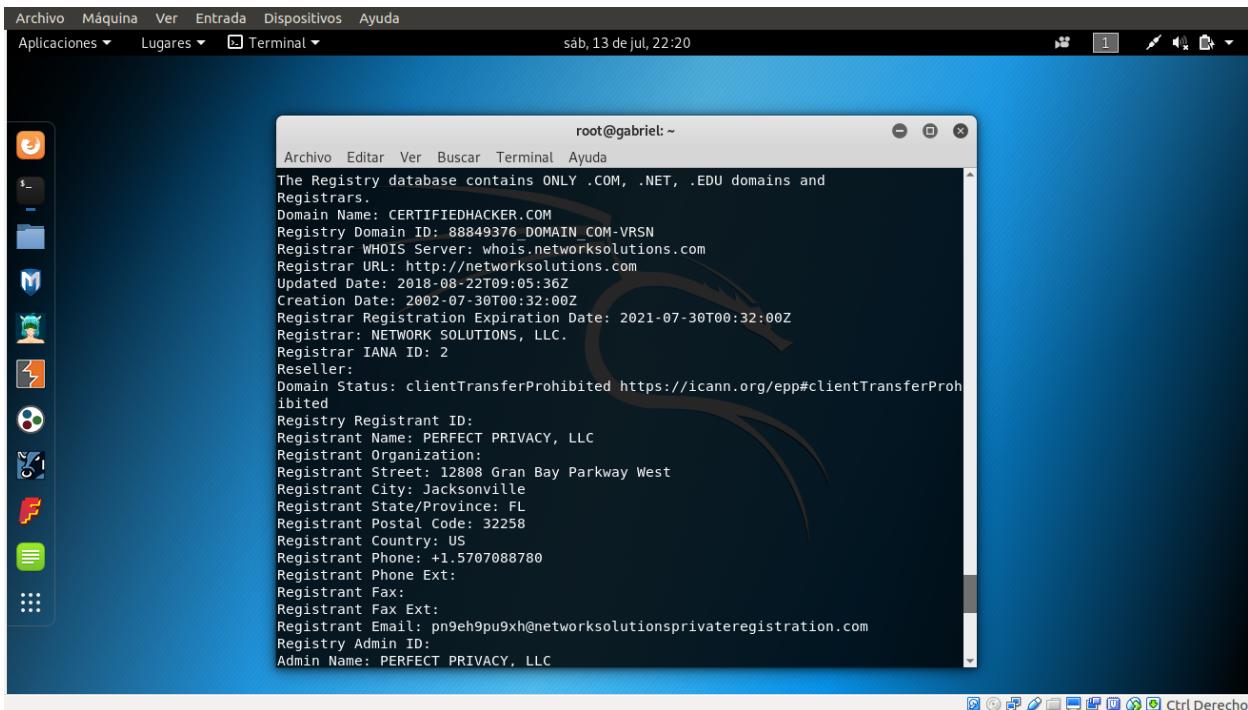
1. Inicie la máquina virtual Kali Linux desde el Administrador de Hyper-V e inicie sesión en ella.
2. Aparece el escritorio de la máquina Kali Linux, como se muestra en la siguiente captura de pantalla.



3. Seleccione **Aplicaciones -> Accessories → Terminal** esto nos lancara 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



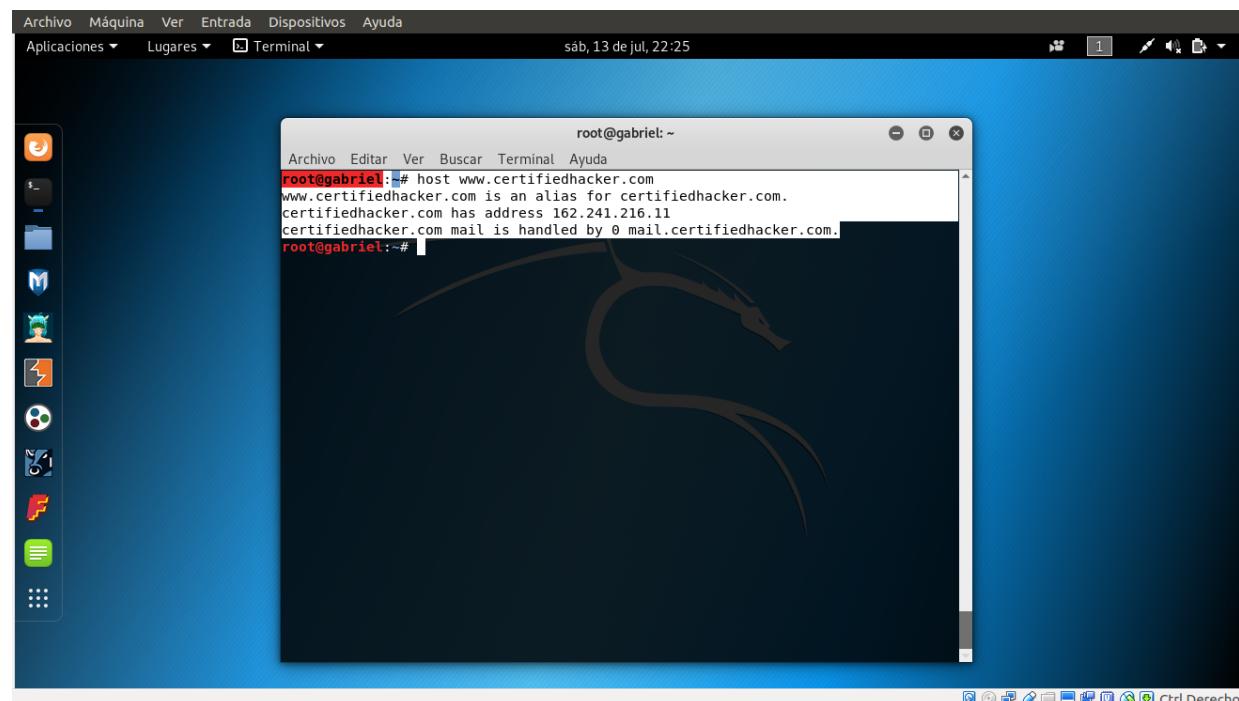
8. Desplácese hacia abajo en la ventana del terminal la información relacionada con el **registrador**.



```
root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-08-22T09:05:36Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2021-07-30T00:32:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 12808 Gran Bay Parkway West
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pn9eh9pu9xh@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
```

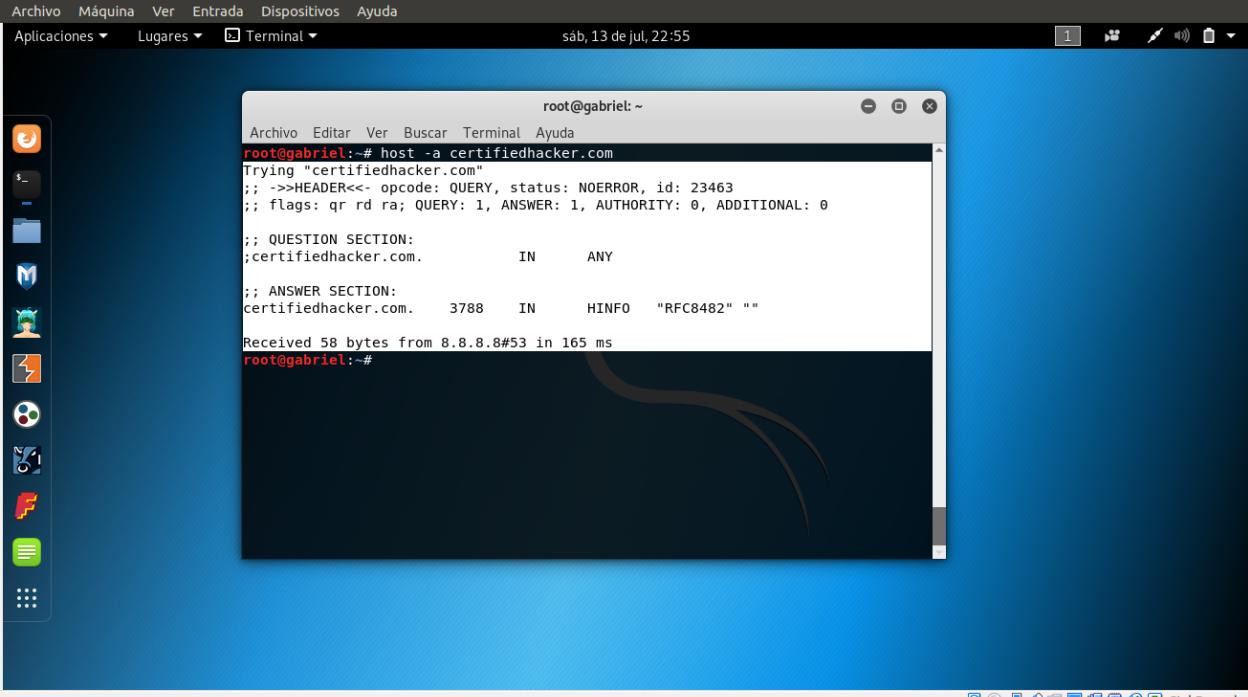
9. Escriba **host certifiedhacker.com** para enumerar la dirección IP del sitio web www.certifiedhacker.com

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



```
root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@gabriel:~# host www.certifiedhacker.com
www.certifiedhacker.com is an alias for certifiedhacker.com.
certifiedhacker.com has address 162.241.216.11
certifiedhacker.com mail is handled by 0 mail.certifiedhacker.com.
root@gabriel:~#
```

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.



A screenshot of a Linux desktop environment. A terminal window titled "root@gabriel: ~" is open, displaying the output of the "host -a certifiedhacker.com" command. The terminal shows the DNS query process, including the question section (certifiedhacker.com. IN ANY), the answer section (certifiedhacker.com. 3788 IN HINFO "RFC8482" ""), and the received response from port 53. The desktop interface includes a vertical application menu on the left, a dock at the bottom with icons for various applications like a browser, file manager, and terminal, and a system tray at the top right.

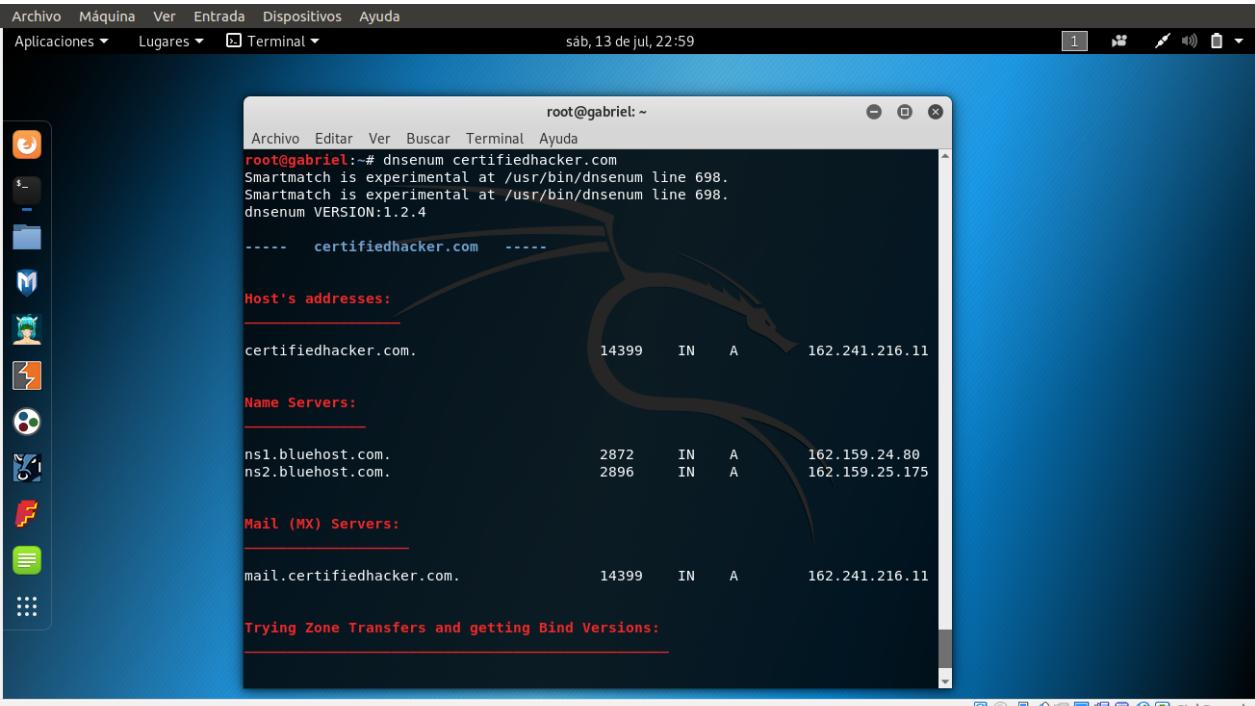
```
root@gabriel:~# host -a certifiedhacker.com
Trying "certifiedhacker.com"
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23463
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;certifiedhacker.com.      IN      ANY

;; ANSWER SECTION:
certifiedhacker.com.    3788    IN      HINFO   "RFC8482"  ""

Received 58 bytes from 8.8.8.8#53 in 165 ms
root@gabriel:~#
```

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.



A screenshot of a Linux desktop environment. A terminal window titled "root@gabriel: ~" is open, displaying the output of the "dnsenum certifiedhacker.com" command. The tool provides detailed information about the target domain, including host addresses, name servers, and mail servers. It also attempts zone transfers and retrieves bind versions. The desktop interface is similar to the previous screenshot, with a vertical application menu, a dock at the bottom, and a system tray at the top right.

```
root@gabriel:~# dnsenum certifiedhacker.com
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4
----- certifiedhacker.com -----
Host's addresses:
-----
certifiedhacker.com.          14399   IN   A   162.241.216.11

Name Servers:
-----
ns1.bluehost.com.            2872    IN   A   162.159.24.80
ns2.bluehost.com.            2896    IN   A   162.159.25.175

Mail (MX) Servers:
-----
mail.certifiedhacker.com.    14399   IN   A   162.241.216.11

Trying Zone Transfers and getting Bind Versions:
-----
```

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.

```
root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda
Host's addresses:
certifiedhacker.com.          14400   IN   A    162.241.216.11

Name Servers:
ns1.bluehost.com.            3596    IN   A    162.159.24.80
ns2.bluehost.com.            3600    IN   A    162.159.25.175

Mail (MX) Servers:
mail.certifiedhacker.com.    14400   IN   A    162.241.216.11

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for certifiedhacker.com on ns1.bluehost.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for certifiedhacker.com on ns2.bluehost.com ...
AXFR record query failed: NOTIMP

brute force file not specified, bay.
root@gabriel: ~#
```

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.

```
root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda
ns2.bluehost.com.            3600    IN   A    162.159.25.175
ns1.bluehost.com.            3600    IN   A    162.159.24.80

Mail (MX) Servers:
mail.certifiedhacker.com.    14400   IN   A    162.241.216.11

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for certifiedhacker.com on ns2.bluehost.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for certifiedhacker.com on ns1.bluehost.com ...
AXFR record query failed: NOTIMP

Brute forcing with /usr/share/dnsenum/dns.txt:
blog.certifiedhacker.com.    14400   IN   A    162.241.216.11
ftp.certifiedhacker.com.     14400   IN   CNAME  certifiedhacker
.com.
certifiedhacker.com.         14400   IN   A    162.241.216.11
mail.certifiedhacker.com.    14400   IN   A    162.241.216.11
root@gabriel: ~#
```

```

root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for certifiedhacker.com on ns2.bluehost.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for certifiedhacker.com on ns1.bluehost.com ...
AXFR record query failed: NOTIMP

Brute forcing with /usr/share/dnsenum/dns.txt:

blog.certifiedhacker.com.          14400   IN    A      162.241.216.11
ftp.certifiedhacker.com.           14400   IN    CNAME  certifiedhacker.com.
certifiedhacker.com.                14400   IN    A      162.241.216.11
mail.certifiedhacker.com.          14400   IN    A      162.241.216.11
news.certifiedhacker.com.          14400   IN    A      162.241.216.11
pop.certifiedhacker.com.            14400   IN    CNAME  mail.certifiedhacker.com.
mail.certifiedhacker.com.          14400   IN    A      162.241.216.11
smtp.certifiedhacker.com.          14400   IN    CNAME  mail.certifiedhacker.com.
mail.certifiedhacker.com.          14332   IN    A      162.241.216.11
webmail.certifiedhacker.com.        14400   IN    A      162.241.216.11
www.certifiedhacker.com.           14400   IN    CNAME  certifiedhacker.com.
certifiedhacker.com.                14400   IN    A      162.241.216.11

certifiedhacker.com class C netrangles:

```

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

```

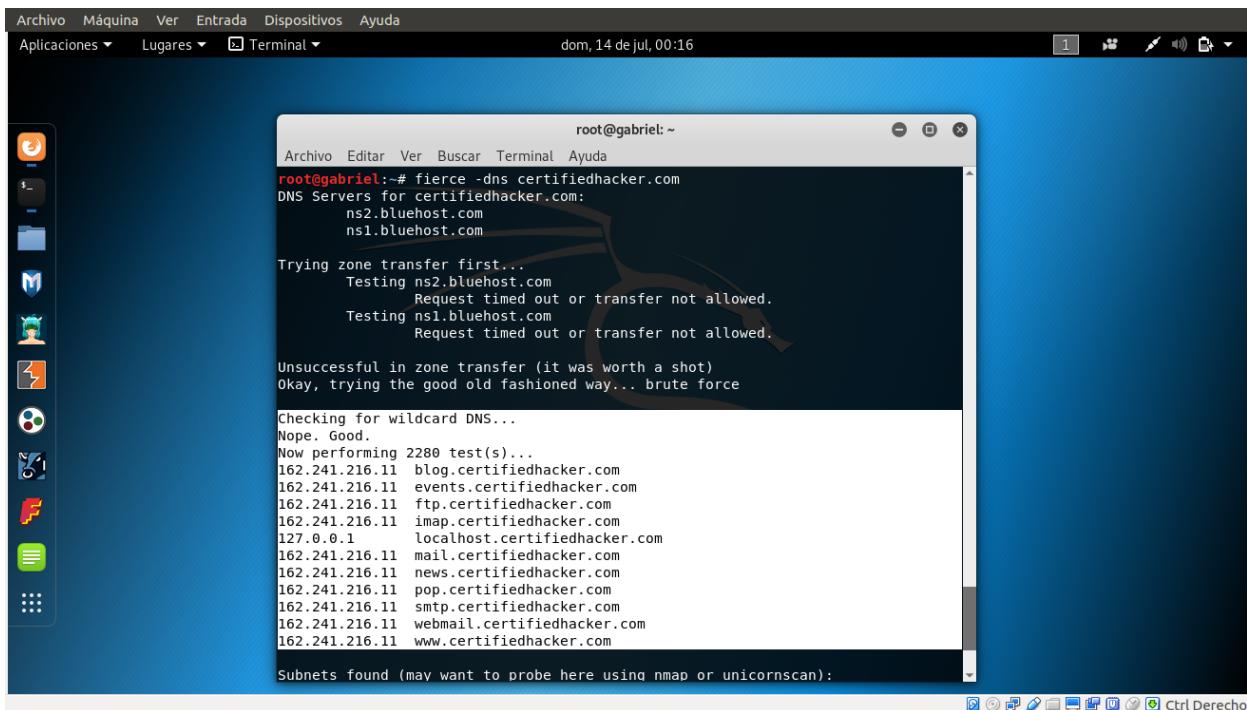
root@gabriel: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@gabriel:~# dnsdict6 -d -4 certifiedhacker.com
Starting DNS enumeration work on certifiedhacker.com. ...
Gathering NS and MX information...
NS of certifiedhacker.com. is ns2.bluehost.com. => 162.159.25.175
NS of certifiedhacker.com. is ns1.bluehost.com. => 162.159.24.80
No IPv6 address for NS entries found in DNS for domain certifiedhacker.com.
MX of certifiedhacker.com. is mail.certifiedhacker.com. => 162.241.216.11
No IPv6 address for MX entries found in DNS for domain certifiedhacker.com.

Starting enumerating certifiedhacker.com. - creating 8 threads for 1420 words...
Estimated time to completion: 1 to 2 minutes
autodiscover.certifiedhacker.com. => 162.241.216.11
blog.certifiedhacker.com. => 162.241.216.11
events.certifiedhacker.com. => 162.241.216.11
ftp.certifiedhacker.com. => 162.241.216.11
imap.certifiedhacker.com. => 162.241.216.11
localhost.certifiedhacker.com. => 127.0.0.1
mail.certifiedhacker.com. => 162.241.216.11
news.certifiedhacker.com. => 162.241.216.11
pop.certifiedhacker.com. => 162.241.216.11
sftp.certifiedhacker.com. => 162.241.216.11
smtp.certifiedhacker.com. => 162.241.216.11
webmail.certifiedhacker.com. => 162.241.216.11
www.certifiedhacker.com. => 162.241.216.11

Found 13 domain names, 2 unique ipv4 and 0 unique ipv6 addresses for certifiedhacker.com.
root@gabriel:~#

```

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.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@gabriel: ~". The terminal content displays the output of the "fierce" command run against the domain "certifiedhacker.com". The output includes:

```
root@gabriel:~# fierce -dns certifiedhacker.com
DNS Servers for certifiedhacker.com:
    ns2.bluehost.com
    ns1.bluehost.com

Trying zone transfer first...
    Testing ns2.bluehost.com
        Request timed out or transfer not allowed.
    Testing ns1.bluehost.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
 Nope. Good.
Now performing 2280 test(s)...
162.241.216.11 blog.certifiedhacker.com
162.241.216.11 events.certifiedhacker.com
162.241.216.11 ftp.certifiedhacker.com
162.241.216.11 imap.certifiedhacker.com
127.0.0.1 localhost.certifiedhacker.com
162.241.216.11 mail.certifiedhacker.com
162.241.216.11 news.certifiedhacker.com
162.241.216.11 pop.certifiedhacker.com
162.241.216.11 smtp.certifiedhacker.com
162.241.216.11 webmail.certifiedhacker.com
162.241.216.11 www.certifiedhacker.com

Subnets found (may want to probe here using nmap or unicornscan):
```