

## Ficha y Control de Resultados de las Prácticas

### Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	11/11/2022
Gabriel Manrique	26921248		
Nombre de la Práctica		Sniffing & Spoofing	
Grupo (últimos 2 dígitos del NRC)		1489	Mesa

### Direccionamiento IP/Máscara:

Equipo origen/fuente:	172.30.114.5	Equipo Objetivo/Destino:	172.30.114.4
Otros Equipos involucrados:			

### Ejecución de la práctica:

Por cada actividad desarrollada durante la ejecución de la práctica debe narrar la(s) actividad(es) llevadas a cabo y colocar las evidencias resultantes, a saber: evidencia de comandos, aplicaciones, programas ejecutados, así como los resultados obtenidos de la ejecución de los mismos:

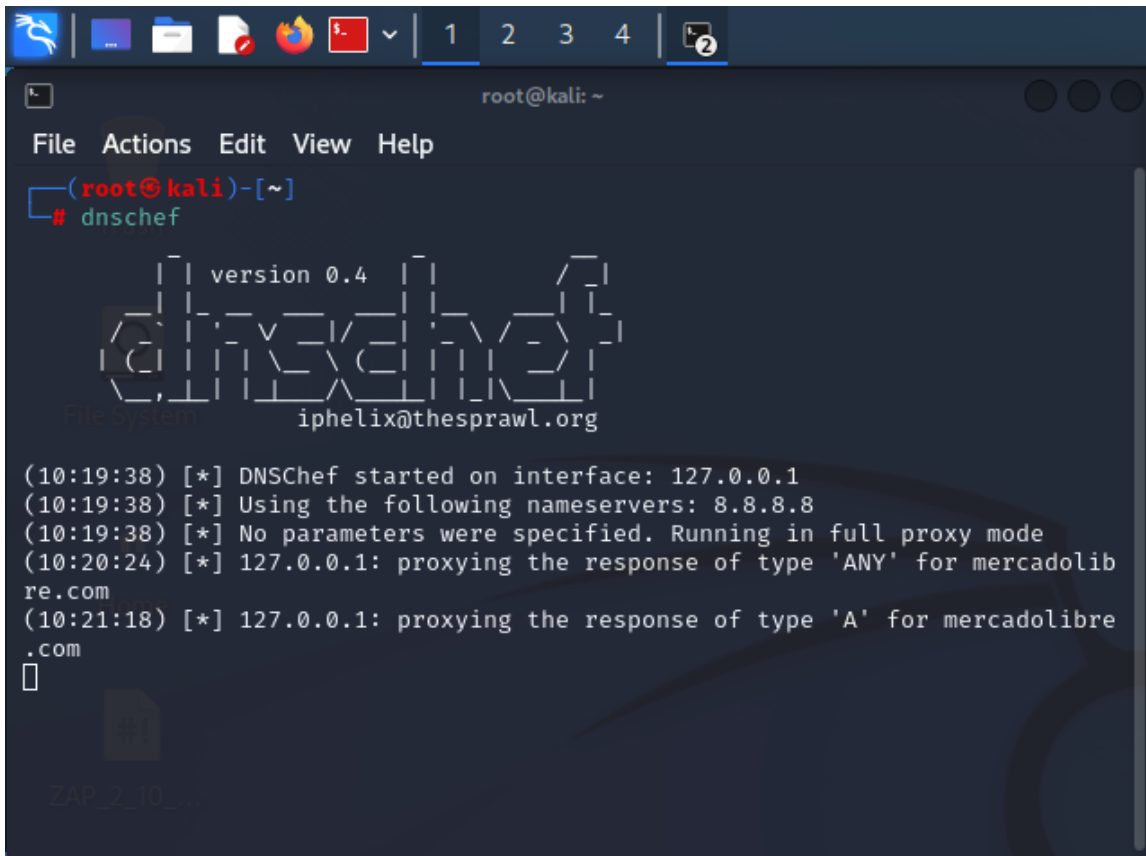
Para la elaboración de esta práctica utilizamos DNSChef una herramienta de kali linux cuyo código fuente se encuentra escrito en Python. Esta herramienta nos permite crear un proxy DNS (Fake DNS) con múltiples configuraciones de una forma sencilla y rápida. Al ser un servidor proxy sirve como filtro registrando la actividad que pasa por él.

Con el uso de DNSChef añadimos uno de los ciberataques más usados, el Sniffing este ciberataque tiene lugar cuando los paquetes que pasan por una red son monitorizados, capturados y, a veces, analizados. En otras palabras, se puede monitorear los url accedidos en un servidor a través de internet. Por otra parte, en conjunto al Sniffing, utilizamos el ciberataque spoofing es un ciberataque que se produce cuando un estafador se hace pasar por un remitente de confianza para acceder a datos o información importantes.

Algunos términos importantes para obtener el mayor conocimiento en la descripción de esta práctica. Servidor **DNS** es el acrónimo de *Domain Name System* o Sistema de Nombres de Dominio, es el método utilizado por Internet para traducir fácilmente los nombres de dominio como *wpseguro.com*, en lugar de su dirección IP 178.33.117.45 de manera que sean entendibles

por los usuarios. Un proxy DNS mejora el rendimiento de la búsqueda de dominio mediante el almacenamiento en caché de las búsquedas anteriores.

Una vez indagamos un poco más en términos técnicos, iniciamos nuestra máquina virtual de kali linux. Nuestro sistema operativo ya trae incluida la herramienta de DNSChef y para confirmarlo ejecutamos el comando **dnscchef**. Con este comando activamos el servidor en nuestro localhost 127.0.0.1.



```

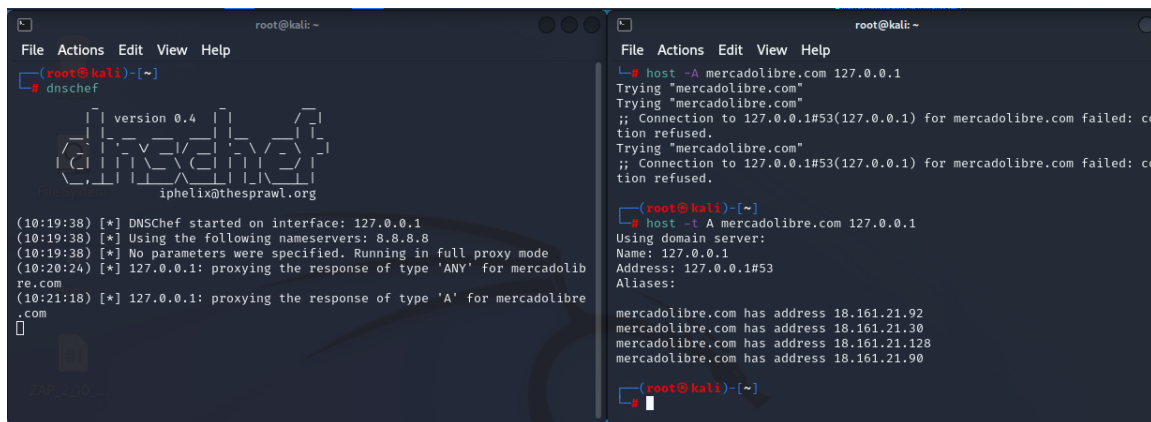
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# dnscchef

[version 0.4]
[File system] iphelix@thesprawl.org

(10:19:38) [*] DNSChef started on interface: 127.0.0.1
(10:19:38) [*] Using the following nameservers: 8.8.8.8
(10:19:38) [*] No parameters were specified. Running in full proxy mode
(10:20:24) [*] 127.0.0.1: proxying the response of type 'ANY' for mercadolib
re.com
(10:21:18) [*] 127.0.0.1: proxying the response of type 'A' for mercadolibre
.com

```

Para la práctica ejecutamos dos ventanas de terminal, en una vamos a activar el servidor proxy con DNSChef y en la otra vamos a realizar las solicitudes. Para hacer una prueba inicial hacemos una consulta a la url de mercado libre con el comando host -t, esto nos permite ver todos los FQDN, Un FQDN sus siglas son Fully Qualified Domain Name es un nombre de dominio completo que incluye el nombre de la computadora y el nombre de dominio asociado.



```

root@kali: ~
File Actions Edit View Help
root@kali)~# dnschef
[+] version 0.4
[+] iphelix@thesprawl.org
(10:19:38) [*] DNSChef started on interface: 127.0.0.1
(10:19:38) [*] Using the following nameservers: 8.8.8.8
(10:19:38) [*] No parameters were specified. Running in full proxy mode
(10:20:24) [*] 127.0.0.1: proxying the response of type 'ANY' for mercadolib
re.com
(10:21:18) [*] 127.0.0.1: proxying the response of type 'A' for mercadolib
re.com

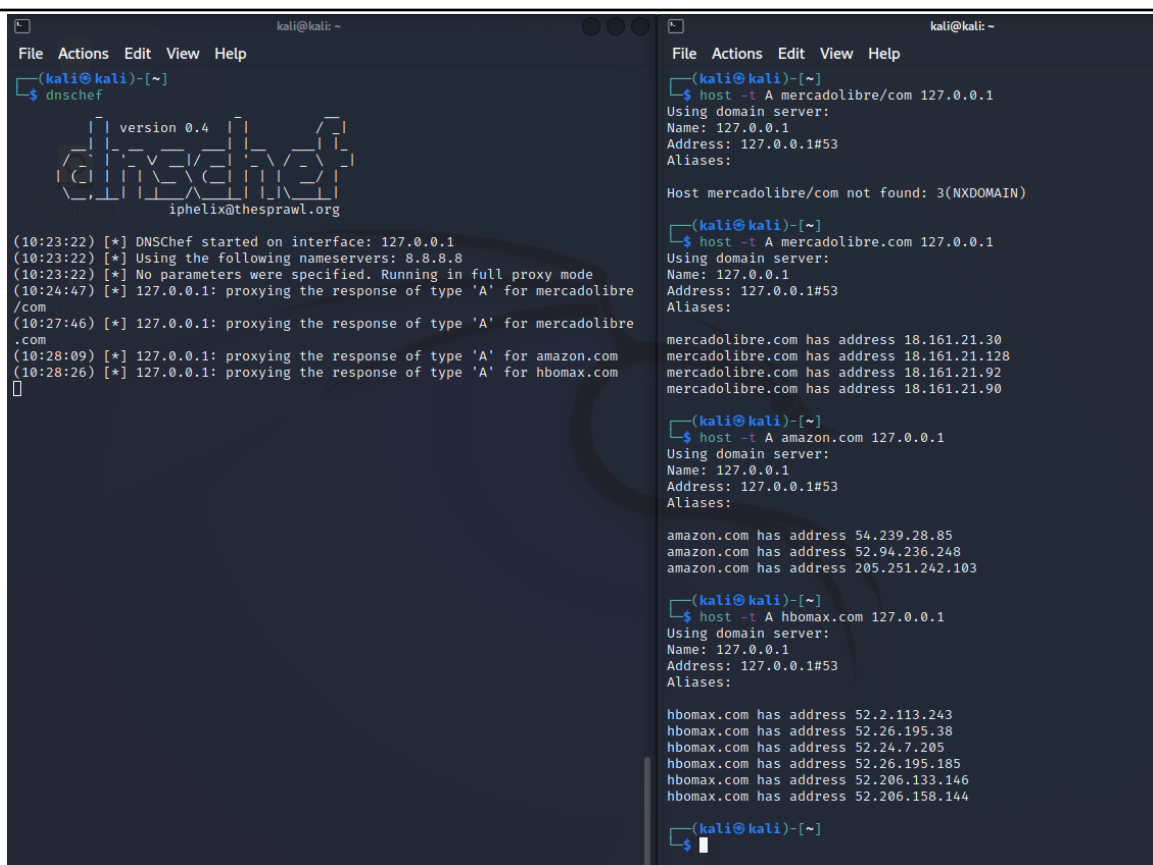
root@kali: ~
File Actions Edit View Help
root@kali)~# host -t A mercadolibre.com 127.0.0.1
Trying "mercadolibre.com"
Trying "mercadolibre.com"
;; Connection to 127.0.0.1#53(127.0.0.1) for mercadolibre.com failed: con
tion refused.
Trying "mercadolibre.com"
;; Connection to 127.0.0.1#53(127.0.0.1) for mercadolibre.com failed: con
tion refused.

root@kali)~# host -t A mercadolibre.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

mercadolibre.com has address 18.161.21.92
mercadolibre.com has address 18.161.21.30
mercadolibre.com has address 18.161.21.128
mercadolibre.com has address 18.161.21.90
root@kali)~#

```

Realizamos el mismo procedimiento pero ahora con las url de hbomax y amazon. Podemos observar como nuestro proxy nos muestra en el terminal del servidor todas y cada una de las consultas que realizamos. Por otro lado, podemos observar la información relacionada a los DNS y direcciones ip de las páginas consultadas.



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ dnschef

  version 0.4
  iphelix@thesprawl.org

(10:23:22) [*] DNSChef started on interface: 127.0.0.1
(10:23:22) [*] Using the following nameservers: 8.8.8.8
(10:23:22) [*] No parameters were specified. Running in full proxy mode
(10:24:47) [*] 127.0.0.1: proxying the response of type 'A' for mercadolibre
/com
(10:27:46) [*] 127.0.0.1: proxying the response of type 'A' for mercadolibre
.com
(10:28:09) [*] 127.0.0.1: proxying the response of type 'A' for amazon.com
(10:28:26) [*] 127.0.0.1: proxying the response of type 'A' for hbomax.com
[]

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ host -t A mercadolibre/com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

Host mercadolibre/com not found: 3(NXDOMAIN)

(kali@kali)-[~]
$ host -t A mercadolibre.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

mercadolibre.com has address 18.161.21.30
mercadolibre.com has address 18.161.21.128
mercadolibre.com has address 18.161.21.92
mercadolibre.com has address 18.161.21.90

(kali@kali)-[~]
$ host -t A amazon.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

amazon.com has address 54.239.28.85
amazon.com has address 52.94.236.248
amazon.com has address 205.251.242.103

(kali@kali)-[~]
$ host -t A hbomax.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

hbomax.com has address 52.2.113.243
hbomax.com has address 52.26.195.38
hbomax.com has address 52.24.7.205
hbomax.com has address 52.26.195.185
hbomax.com has address 52.206.133.146
hbomax.com has address 52.206.158.144

(kali@kali)-[~]
$
  
```

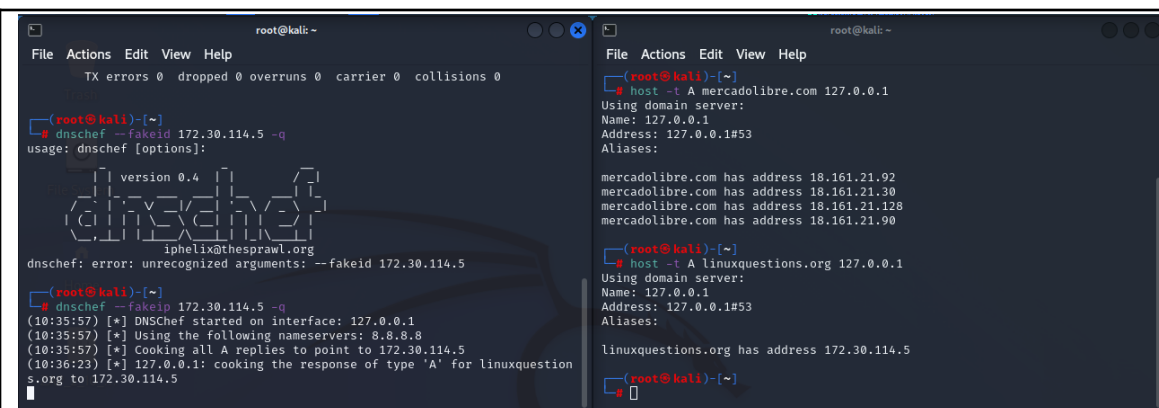
Ahora que sabemos que es la herramienta DNSChef, procedimos a realizar un spoofing de forma práctica. En la siguiente imagen activamos un servidor con un fakeid, la cual será la dirección ip de nuestra máquina virtual.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.114.5 netmask 255.255.255.0 broadcast 172.30.114.255
    inet6 fe80::a00:27ff:feb6:df0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b6:0d:f0 txqueuelen 1000 (Ethernet)
    RX packets 29943 bytes 36738449 (35.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23031 bytes 5545598 (5.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 755 (755.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 755 (755.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ dnscraf --fakeip 172.30.114.5 -q
(10:34:02) [*] DNSChef started on interface: 127.0.0.1
(10:34:02) [*] Using the following nameservers: 8.8.8.8
(10:34:02) [*] Cooking all A replies to point to 172.30.114.5
(10:34:26) [*] 127.0.0.1: cooking the response of type 'A' for linuxquestion
s.org to 172.30.114.5
(10:36:07) [*] 127.0.0.1: cooking the response of type 'A' for disneyplus.co
m to 172.30.114.5
(10:37:26) [*] 127.0.0.1: cooking the response of type 'A' for google.com to
172.30.114.5
█
```

Probamos la conexión y podemos observar que al ejecutar el comando “host -t A” a la url de linuxquestions.org 127.0.0.1, obtuvimos un resultado en el cual la dirección ip del dominio es la dirección de nuestra máquina.



```

root@kali:~
File Actions Edit View Help
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# dnschef --fakeip 172.30.114.5 -q
usage: dnschef [options]:

version 0.4
iphelix@thesprawl.org
dnschef: error: unrecognized arguments: --fakeip 172.30.114.5

root@kali:~# dnschef --fakeip 172.30.114.5 -q
(10:35:57) [*] DNSChuf started on interface: 127.0.0.1
(10:35:57) [*] Using the following nameservers: 8.8.8.8
(10:35:57) [*] Cooking all A replies to point to 172.30.114.5
(10:36:23) [*] 127.0.0.1: cooking the response of type 'A' for linuxquestion
s.org to 172.30.114.5

root@kali:~# host -t A mercadolibre.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

mercadolibre.com has address 18.161.21.92
mercadolibre.com has address 18.161.21.30
mercadolibre.com has address 18.161.21.128
mercadolibre.com has address 18.161.21.90

root@kali:~# host -t A linuxquestions.org 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

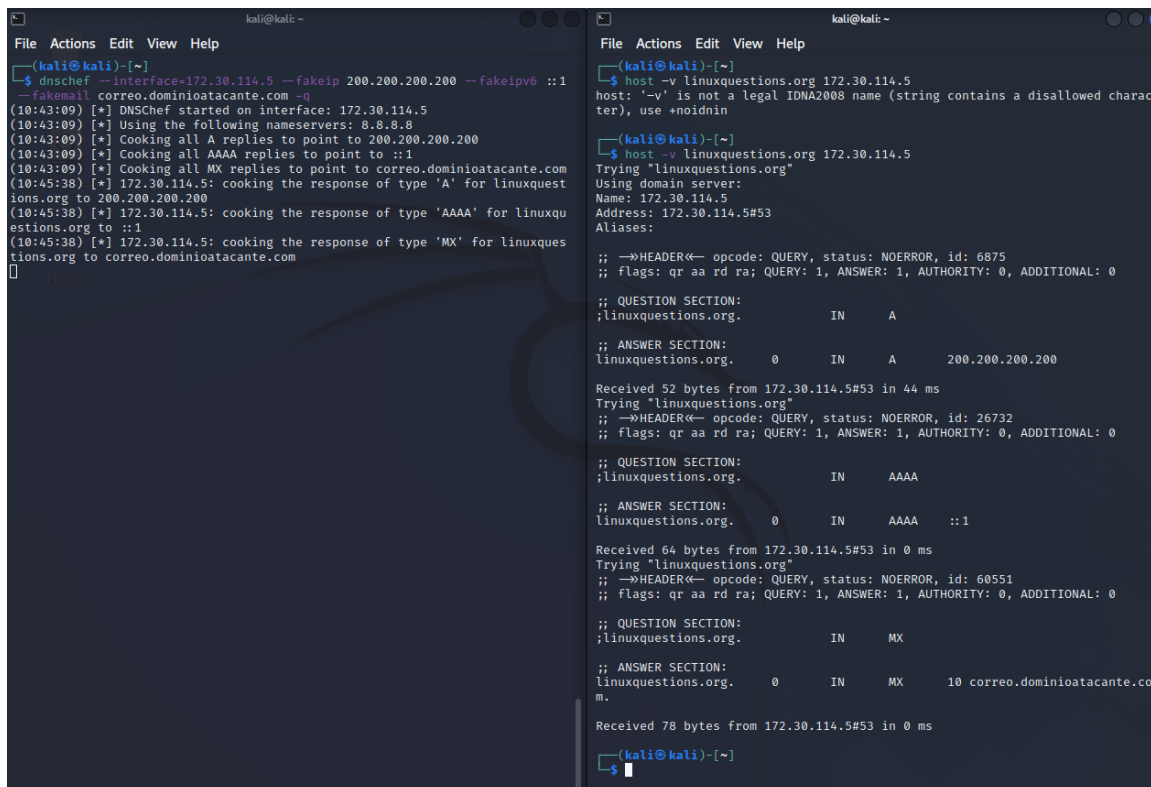
linuxquestions.org has address 172.30.114.5

root@kali:~#

```

Para hacer una prueba exhaustiva con parámetros específicos para la configuración del servidor proxy como la dirección Ipv4, el servicio de correo y la dirección Ipv6; Definimos en el comando de la siguiente manera detallando la interfaz igual a la ip de nuestra maquina 172.30.114.5, el fakeip 200.200.200.200, fakeipv6 ::1 y fakemail correo.dominioatacante.com, como se muestra en la imagen.

Como se puede observar en la imagen anterior en el terminal de peticiones, la información que nos retorna el servidor, después de ejecutar el comando **host -v linuxquestions.org 172.30.114.5**, es la relacionada a nuestros hyperparametro definidos en el proxy. Mientras que el terminal servidor registra las consultas.



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ dnschef --interface=172.30.114.5 --fakeip 200.200.200.200 --fakeip6 ::1
--fakemail correo.dominioatacante.com -q
(10:43:09) [*] DNSChef started on interface: 172.30.114.5
(10:43:09) [*] Using the following nameservers: 8.8.8.8
(10:43:09) [*] Cooking all A replies to point to 200.200.200.200
(10:43:09) [*] Cooking all AAAA replies to point to ::1
(10:43:09) [*] Cooking all MX replies to point to correo.dominioatacante.com
(10:45:38) [*] 172.30.114.5: cooking the response of type 'A' for linuxquestions.org to 200.200.200.200
(10:45:38) [*] 172.30.114.5: cooking the response of type 'AAAA' for linuxquestions.org to ::1
(10:45:38) [*] 172.30.114.5: cooking the response of type 'MX' for linuxquestions.org to correo.dominioatacante.com
[]

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ host -v linuxquestions.org 172.30.114.5
host: '-v' is not a legal IDNA2008 name (string contains a disallowed character), use +noidn
(kali@kali)-[~]
$ host -v linuxquestions.org 172.30.114.5
Trying "linuxquestions.org"
Using domain server:
Name: 172.30.114.5
Address: 172.30.114.5#53
Aliases:

;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 6875
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;linuxquestions.org.          IN      A

;; ANSWER SECTION:
linuxquestions.org.  0      IN      A      200.200.200.200

Received 52 bytes from 172.30.114.5#53 in 44 ms
Trying "linuxquestions.org"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 26732
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;linuxquestions.org.          IN      AAAA

;; ANSWER SECTION:
linuxquestions.org.  0      IN      AAAA      ::1

Received 64 bytes from 172.30.114.5#53 in 0 ms
Trying "linuxquestions.org"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 60551
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;linuxquestions.org.          IN      MX

;; ANSWER SECTION:
linuxquestions.org.  0      IN      MX      10 correo.dominioatacante.com.

Received 78 bytes from 172.30.114.5#53 in 0 ms
(kali@kali)-[~]
$

```

Realizamos el procedimiento anterior con la url de **disneyplus** y **amazon**. Los resultados serán los mismos siempre que coloquemos la dirección del servidor dns **172.30.114.5** que creamos.

```
(kali㉿kali)-[~]
$ host -v amazon.com 172.30.114.5
Trying "amazon.com"
Using domain server:
Name: 172.30.114.5
Address: 172.30.114.5#53
Aliases:

;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 45822
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      A

;; ANSWER SECTION:
amazon.com.                 0      IN      A      200.200.200.200

Received 44 bytes from 172.30.114.5#53 in 0 ms
Trying "amazon.com"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 50598
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      AAAA

;; ANSWER SECTION:
amazon.com.                 0      IN      AAAA    ::1

Received 56 bytes from 172.30.114.5#53 in 4 ms
Trying "amazon.com"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 18529
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      MX

;; ANSWER SECTION:
amazon.com.                 0      IN      MX      10 correo.dominioatacante.co
m.

Received 67 bytes from 172.30.114.5#53 in 0 ms
```



```

kali@kali: ~
File Actions Edit View Help
$ dnscatf --interface=172.30.114.5 --fakeip 200.200.200.200 --fakeip6 ::1
--fakeip correo.dominioatacante.com -q
(10:43:09) [*] Dnscatf started on interface: 172.30.114.5
(10:43:09) [*] Using the following nameservers: 8.8.8.8
(10:43:09) [*] Cooking all A replies to point to 200.200.200.200
(10:43:09) [*] Cooking all AAAA replies to point to ::1
(10:43:09) [*] Cooking all MX replies to point to correo.dominioatacante.com
(10:45:38) [*] 172.30.114.5: cooking the response of type 'A' for linuxquest
ions.org to 200.200.200.200
(10:45:38) [*] 172.30.114.5: cooking the response of type 'AAAA' for linuxqu
estions.org to ::1
(10:45:38) [*] 172.30.114.5: cooking the response of type 'MX' for linuxques
tions.org to correo.dominioatacante.com
(10:46:31) [*] 172.30.114.5: cooking the response of type 'A' for disneyplus
.com to 200.200.200.200
(10:46:31) [*] 172.30.114.5: cooking the response of type 'AAAA' for disneypl
us.com to ::1
(10:46:31) [*] 172.30.114.5: cooking the response of type 'MX' for disneyplu
s.com to correo.dominioatacante.com
[]

kali@kali: ~
File Actions Edit View Help
;; ANSWER SECTION:
linuxquestions.org. 0 IN MX 10 correo.dominioatacante.co
m.

Received 78 bytes from 172.30.114.5#53 in 0 ms

kali@kali: ~
$ host -v disneyplus.com 172.30.114.5
Trying "disneyplus.com"
Using domain server:
Name: 172.30.114.5
Address: 172.30.114.5#53
Aliases:

;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 26644
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;disneyplus.com. IN A

;; ANSWER SECTION:
disneyplus.com. 0 IN A 200.200.200.200

Received 48 bytes from 172.30.114.5#53 in 0 ms
Trying "disneyplus.com"
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 4416
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;disneyplus.com. IN AAAA

;; ANSWER SECTION:
disneyplus.com. 0 IN AAAA ::1

Received 60 bytes from 172.30.114.5#53 in 4 ms
Trying "disneyplus.com"
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 62655
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;disneyplus.com. IN MX

;; ANSWER SECTION:
disneyplus.com. 0 IN MX 10 correo.dominioatacante.co
m.

Received 71 bytes from 172.30.114.5#53 in 0 ms

```

Para comprobar cuál es la información real de los url hicimos la prueba con el dns de google y la página de amazon. Debido a esto podemos determinar las Ipv4, Ipv6, el correo de amazon entre otras cosas.

```
(kali@kali)-[~]
$ host -v amazon.com 8.8.8.8
Trying "amazon.com"
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 57247
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      A

;; ANSWER SECTION:
amazon.com.        667     IN      A      54.239.28.85
amazon.com.        667     IN      A      205.251.242.103
amazon.com.        667     IN      A      52.94.236.248

Received 76 bytes from 8.8.8.8#53 in 36 ms
Trying "amazon.com"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 30162
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      AAAA

;; AUTHORITY SECTION:
amazon.com.        11      IN      SOA     dns-external-master.amazon.c
om. root.amazon.com. 2010163719 180 60 3024000 60

Received 89 bytes from 8.8.8.8#53 in 36 ms
Trying "amazon.com"
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 26237
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;amazon.com.                IN      MX

;; ANSWER SECTION:
amazon.com.        723     IN      MX      5 amazon-smtp.amazon.com.

Received 56 bytes from 8.8.8.8#53 in 44 ms
```

### Referencias Bibliográficas

<https://nordvpn.com/es/blog/sniffer-que-es/>  
<https://www.pandasecurity.com/es/mediacenter/seguridad/que-es-el-spoofing/>  
<https://kalilinux.foroactivo.com/t92-tutorial-dnscchef-para-kali-linux>  
<https://www.ionos.es/digitalguide/dominios/gestion-de-dominios/fully-qualified-domain-name/>  
[https://www.reydes.com/d/?q=Utilizar\\_DNSChef\\_para\\_Crear\\_un\\_DNS\\_Falso](https://www.reydes.com/d/?q=Utilizar_DNSChef_para_Crear_un_DNS_Falso)

### **Hallazgos y/o conclusiones de la actividad desarrollada (Explique su experiencia y el análisis de los resultados):**

La finalidad de esta investigación es poner en práctica la aplicación DNSChef como una herramienta altamente utilizada para pruebas de penetración, análisis de malware, entre otras; mejorando así el rendimiento de la búsqueda de dominio, debido a que nos permite crear una capa de abstracción con respecto a la información real del Sistema del nombre de dominio que use una página web y nuestro servidor proxy con información falsa.

Con la ejecución `host -t A` en el terminal se consulta a las páginas web, para observar la información relacionada a los DNS y direcciones IP de las páginas consultadas.

Se realizó un spoofing para activar un servidor con un fakeid, que provoca la redirección de consultas de las páginas web, con la finalidad de dirigirse a una dirección IP falsa.

Por último se realizó un sniffing para monitorear la información de las consultas de páginas web en el servidor.

Gracias a esto se puede redirigir a la víctima a una trampa, realizar ataques de spoofing, sniffing y analizar la red.

**Contribución de esta actividad en su Proyecto:**

Con la creación del fake id, podremos observar y monitorear las consultas de páginas web, que puede realizar la empresa, además de poder redireccionar a una dirección IP específica las consultas hechas por los usuarios.