



Administración de servidores

D05

Vi-Sa 7-9 Hrs

José de Jesús Soto Sánchez



#### Actividad 4 – DNS

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

2023A

En la actividad número 4 de la materia, se necesita instalar el servicio principal para realizar actividades dentro del Internet dentro de nuestro servidor de Linux debian, de manera que sea funcional y que cumpla sus actividades principales, a este servicio se le conoce como protocolo de DNS, es un protocolo que funciona de manera similar a tener un directorio con números de teléfonos por lo que es una base de datos que contiene una amplia cantidad de nombres de los dominios y que facilita su búsqueda entre los usuarios y facilita su conexión con el host para obtener la página o dominio deseado, pero se necesita definir que es el protocolo para poder utilizarlo e instalarlo dentro del servidor.

¿Qué es el DNS?

Por sus siglas en inglés Domain Name System (DNS), en español como Sistema de Nombres de Dominios, es un conjunto de protocolos que funcionan como una base de datos que contiene nombres los cuales son pasados a un proceso de localización y su posterior traducción al Protocolo de Internet (IP), esto para facilitar la búsqueda por nombres en vez de por IPs, de manera que se asigna un nombre a una dirección IP, esto debido a que la mayoría de las actividades dentro del Internet como lo es la búsqueda de la web utilizan el DNS, ya que este servicio conecta rápidamente con la información necesaria para conectar al usuario con el host.

Servidor primario:

Un servidor primario de DNS, es un servidor donde se guarda el archivo de zona principal, el cual es un archivo de base de datos que contiene la información para el dominio, como lo es la IP y otros recursos relevantes para el dominio.

Servidor secundario:

El o los servidores secundarios del DNS contiene la información de los archivos en modo de copia, los cuales solo sirven para consultar información. (cloudflare, 2023)

DNS recursivo e iterativo

En una búsqueda recursiva el servidor de DNS se comunica con varios servidores DNS para encontrar lo que se buscó, en este caso la IP y devolverla al cliente. Mientras que, en una iterativa, el cliente se comunica con cada servidor de DNS que esté relacionado a la búsqueda. (cloudflare, cloudflare, 2023)

Funcionamiento


El servicio de DNS localiza para después traduce, es decir, convierte la URL y el nombre del dominio ingresados por el usuario en el buscador y después los convierte en dirección IP con el objetivo de que las computadoras puedan entender y de ese modo, usar.

Los procesos por los que pasa el protocolo son:

- El usuario debe ingresar la dirección web.
- El buscador envía un mensaje a la red para encontrar cual IP es la correspondiente.
- La consulta va al servidor DNS, si este servidor tiene la dirección la envía.
- En cambio, si no la tiene, se consultan otros servidores como el DNS root entre otros que trabajan para encontrar y devolver lo que el usuario haya ingresado y cargar la página final.
- Sin embargo, si no encuentra nada, entonces devolverá un mensaje de error.

(Lutkevich, 2021)

Con el comando de apt install bind9 dnsutils dentro de usuario root, se descarga e instala el servicio de bind9.

A terminal window titled 'fernando@debian: ~' with search, menu, and close buttons. The user 'fernando@debian' runs 'su -' to become root. Then, 'apt install bind9 dnsutils' is executed. The terminal shows the progress: reading package lists, creating dependency trees, and reading state information, all marked as 'Hecho'. It lists additional packages to be installed: 'bind9-utils' and 'python3-ply'. Suggested packages include 'bind-doc', 'resolvconf', 'ufw', 'python-ply-doc'. It states that 4 new packages will be installed, 0 will be upgraded, and 0 will be removed. The total download size is 1,263 kB, and the additional disk space required is 2,629 kB. It asks for confirmation to continue, which is answered with 'S'. The progress bar shows '0% [Esperando las cabeceras]' with a cursor.

```
fernando@debian:~$ su -
Contraseña:
root@debian:~# apt install bind9 dnsutils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bind9-utils python3-ply
Paquetes sugeridos:
  bind-doc resolvconf ufw python-ply-doc
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-utils dnsutils python3-ply
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 18 no actualizados.
Se necesita descargar 1 263 kB de archivos.
Se utilizarán 2 629 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
0% [Esperando las cabeceras]
```

Después de la instalación de los paquetes adicionales, se modifica el archivo  
/etc/bind/named.conf.local

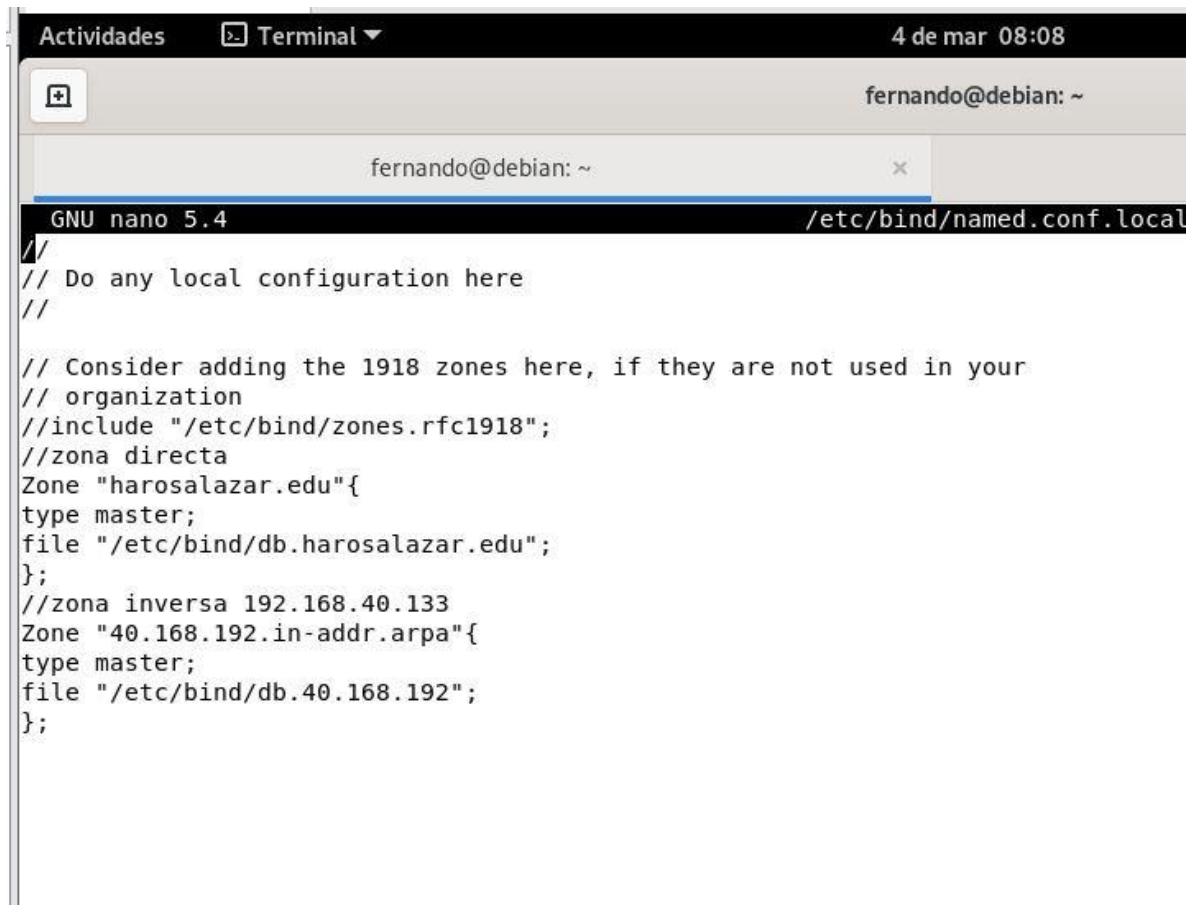
A terminal window showing the user 'root@debian' using the 'nano' text editor to edit the file '/etc/bind/named.conf.local'. The command 'nano /etc/bind/named.conf.local' is entered twice, and the prompt returns to the root shell.

```
root@debian:~# nano named.conf.local
root@debian:~# nano /etc/bind/named.conf.local
root@debian:~#
```

Ya en el interior de este archivo, se agregan líneas como lo es la zona de dominio el cual es harosalazar.edu y los tres primeros números de IP de manera inversa en la zona inversa para definir la búsqueda inversa



```
fernando@debian: ~
GNU nano 5.4 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```



```
Actividades Terminal 4 de mar 08:08
fernando@debian: ~
fernando@debian: ~
GNU nano 5.4 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//zona directa
Zone "harosalazar.edu"{
type master;
file "/etc/bind/db.harosalazar.edu";
};
//zona inversa 192.168.40.133
Zone "40.168.192.in-addr.arpa"{
type master;
file "/etc/bind/db.40.168.192";
};
```

Después de guardar el archivo se comprueba, se crea el archivo en la zona directa, el cual también se modifica con nano

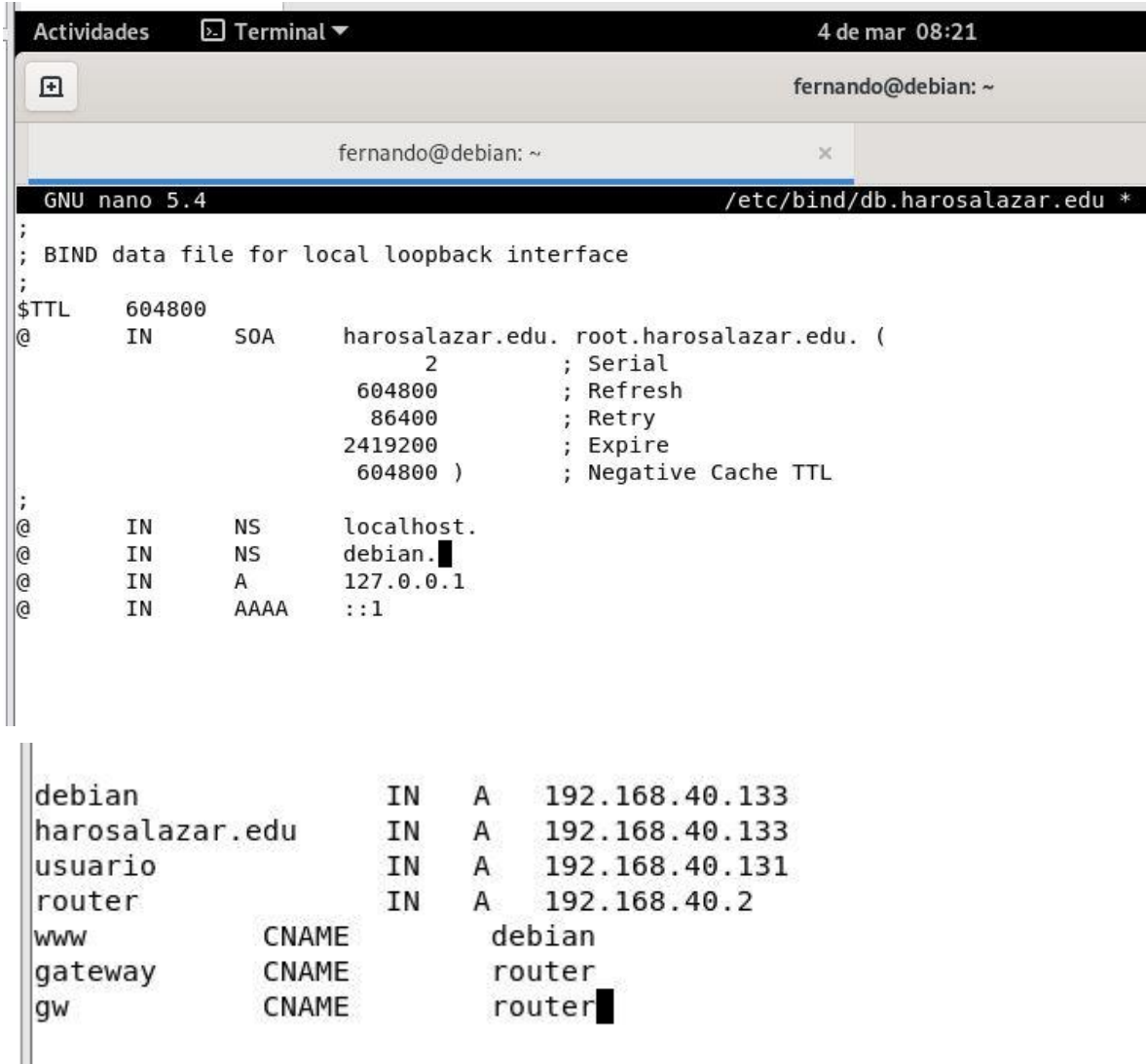
```

root@debian:~# nano /etc/bind/named.conf.local
root@debian:~# named-checkconf
root@debian:~# █

root@debian:~# named-checkconf
root@debian:~# cp /etc/bind/db.local /etc/bind/db.harosalazar.edu
root@debian:~# █

```

En este archivo se realiza una serie de configuraciones como es agregar el nombre del dominio, el nombre del servidor y el nombre del windows



```

GNU nano 5.4 /etc/bind/db.harosalazar.edu *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      harosalazar.edu. root.harosalazar.edu. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       debian.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1

debian            IN      A      192.168.40.133
harosalazar.edu  IN      A      192.168.40.133
usuario          IN      A      192.168.40.131
router           IN      A      192.168.40.2
www              CNAME     debian
gateway          CNAME     router
gw               CNAME     router

```

con named-checkzone se comprueba que la configuración este correcta

```
root@debian:~# named-checkzone harosalazar.edu /etc/bind/db.harosalazar.edu
zone harosalazar.edu/IN: loaded serial 2
OK
root@debian:~#
```

mouse pointer inside or press Ctrl+G.

Desde la terminal se crea un archivo de la zona inversa

A screenshot of a terminal window titled 'fernando@debian: ~'. The terminal shows the following commands and output:   
1. 'fernando@debian:~\$ su -' followed by 'Contraseña:' (password prompt).   
2. 'root@debian:~# cp /etc/bind/db.127 /etc/bind/db.40.168.192'   
3. 'root@debian:~# nano /etc/bind/db.40.168.192'   
4. The nano editor interface appears with the message 'Use «fg» para volver a nano.'   
5. '[1]+ Detenido nano /etc/bind/db.40.168.192'   
6. 'root@debian:~# nano /etc/bind/db.40.168.192'   
7. 'root@debian:~#' followed by a cursor.   
The terminal window has a standard Linux desktop environment header with search, menu, and close buttons.

Se ingresa con nano al archivo creado de la zona inversa y se edita, se agrega el nombre del servidor, así como el último número de la IP de cada máquina virtual acompañada con su nombre de servidor y su dominio.

```
fernando@debian: ~  
GNU nano 5.4 /etc/bind/db.40.168.192  
;  
; BIND reverse data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      localhost. root.localhost. (  
                                1          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )   ; Negative Cache TTL  
;  
@         IN      NS       localhost.  
@         IN      NS       debian.  
1.0.0     IN      PTR      localhost.  
133       IN      PTR      debian.harosalazar.edu.  
131       IN      PTR      Windows7.harosalazar.edu  
1         IN      PTR      router.harosalazar.edu  
[ 18 líneas leídas ]  
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^_ Ir a línea
```

Este comando se usa para verificar que la configuración sea correcta

```
fernando@debian: ~  
root@debian:~# named-checkzone 40.168.192.in-addr.arpa /etc/bind/db.40.168.192  
zone 40.168.192.in-addr.arpa/IN: loaded serial 1  
OK  
root@debian:~#
```

Con nano se configura los forwarders, las cuales son direcciones IP que el DNS consulta cuando no puede resolver una dirección localmente

```
fernando@debian: ~  
root@debian:~# nano /etc/bind/named.conf.options  
root@debian:~#
```

Se cambia el

forwarders a 8.8.8.8, es decir google



```
fernando@debian: ~
GNU nano 5.4 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
[ 24 líneas leídas ]
^G Ayuda    ^O Guardar  ^W Buscar   ^K Cortar   ^T Ejecutar ^C Ubicación
^X Salir    ^R Leer fich.^_ Reemplazar^U Pegar     ^J Justificar^_ Ir a línea
```

```
fernando@debian: ~
GNU nano 5.4 /etc/bind/named.conf.options *
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

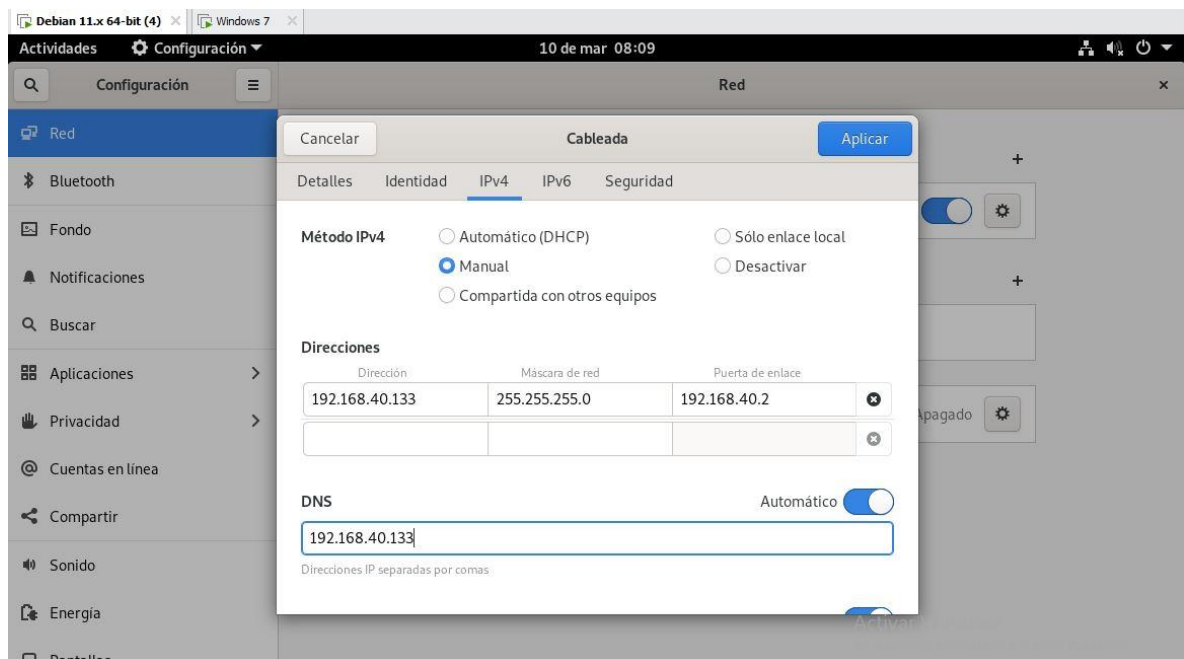
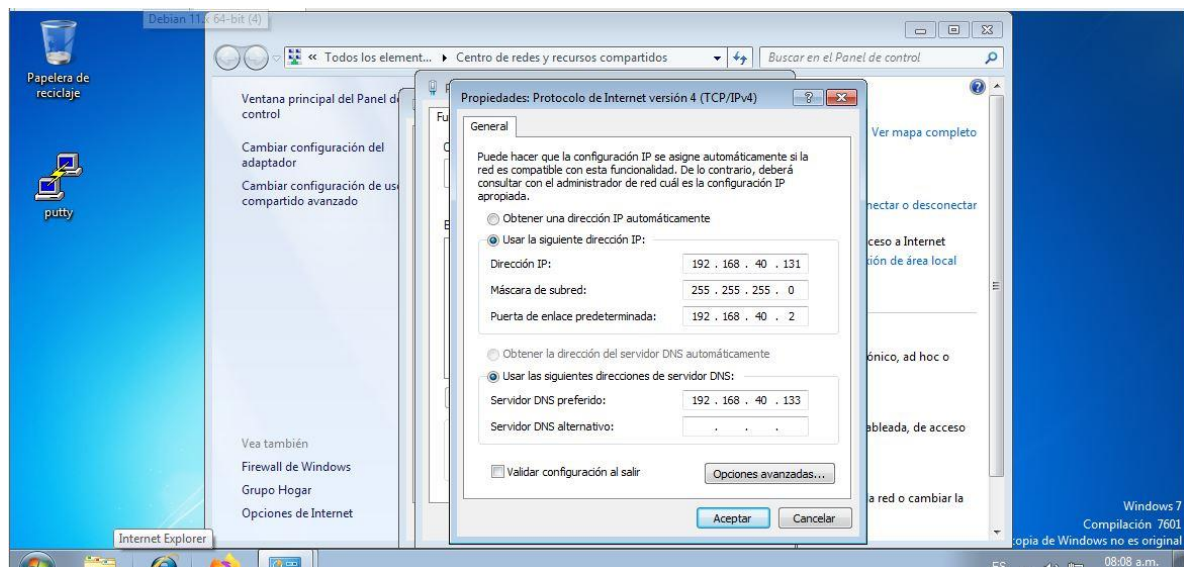
    listen-on-v6 { any; };
};

^G Ayuda    ^O Guardar  ^W Buscar   ^K Cortar   ^T Ejecutar ^C Ubicación
^X Salir    ^R Leer fich.^_ Reemplazar^U Pegar     ^J Justificar^_ Ir a línea
```

Con /etc/init.d/bind9 restart se reinicia el servicio de bind9, pero primero se comprueba o cambia en la tarjeta de red los valores para el DNS cambiando las IP actuales por la de

```
fernando@debian: ~  
root@debian:~# nano /etc/bind/named.conf.options  
root@debian:~# nano /etc/bind/named.conf.options  
root@debian:~# service bind9 restart
```

Debian



Dentro de la terminal de Linux Debian o Windows, se usa el comando nslookup para probar la respuesta DNS a las peticiones por nombre a los diferentes equipos y un dominio de internet, como lo es el propio debian, Windows y google



```
fernando@debian:~$ su -
Contraseña:
root@debian:~# nslookup debian.harosalazar.edu
Server:      192.168.40.133
Address:     192.168.40.133#53

Name:   debian.harosalazar.edu
Address: 192.168.40.133

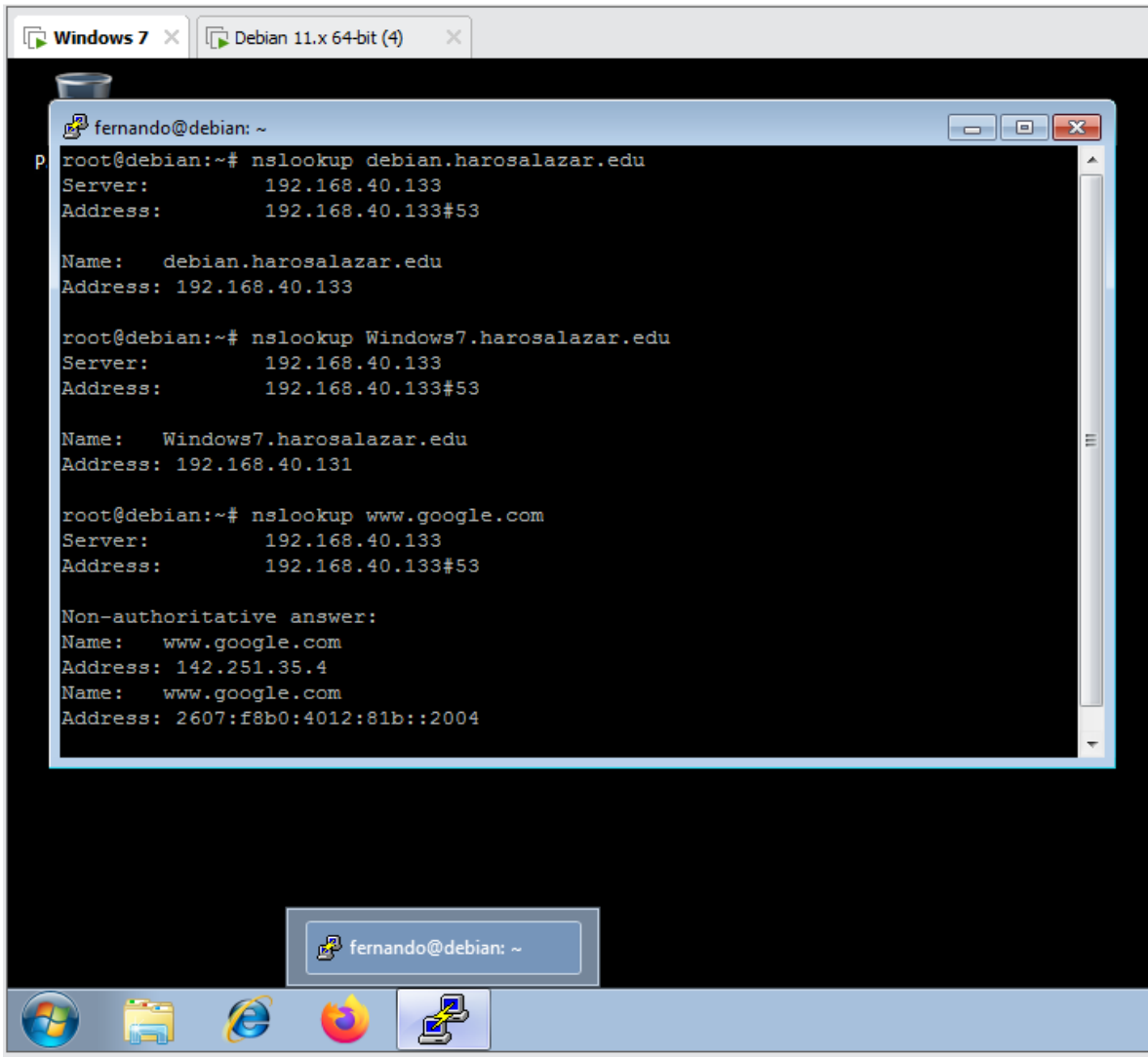
root@debian:~# nslookup Windows7.harosalazar.edu
Server:      192.168.40.133
Address:     192.168.40.133#53

Name:   Windows7.harosalazar.edu
Address: 192.168.40.131

root@debian:~# nslookup www.google.com
Server:      192.168.40.133
Address:     192.168.40.133#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.193.132
Name:   www.google.com
Address: 2607:f8b0:4000:808::2004

root@debian:~#
```



```
C:\Users\usuario>nslookup debian.harosalazar.edu
Servidor:  debian.harosalazar.edu
Address:   192.168.40.133

Nombre:    debian.harosalazar.edu
Address:   192.168.40.133

C:\Users\usuario>nslookup Windows7.harosalazar.edu
Servidor:  debian.harosalazar.edu
Address:   192.168.40.133

Nombre:    Windows7.harosalazar.edu
Address:   192.168.40.131

C:\Users\usuario>nslookup www.google.com
Servidor:  debian.harosalazar.edu
Address:   192.168.40.133

Respuesta no autoritativa:
Nombre:    www.google.com
Addresses: 2607:f8b0:4012:81b::2004
          142.251.35.4
```

```
fernando@debian: ~  
fernando@debian:~$ su -  
Contraseña:  
root@debian:~# ping debian.harosalazar.edu  
PING debian.harosalazar.edu (127.0.1.1) 56(84) bytes of data.  
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=1 ttl=64 time=0.046 m  
s  
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=2 ttl=64 time=0.080 m  
s  
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=3 ttl=64 time=0.064 m  
s  
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=4 ttl=64 time=0.041 m  
s
```

Por medio del putty de Windows y de la terminal, se compueba la respuesta del DNS

```
Windows 7 x Debian 11.x 64-bit (4)  
fernando@debian: ~  
root@debian:~# dig @8.8.8.8 google.com  
  
; <<>> DiG 9.16.37-Debian <<>> @8.8.8.8 google.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63182  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;google.com. IN A  
  
;; ANSWER SECTION:  
google.com. 46 IN A 142.251.34.46  
  
;; Query time: 91 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8)  
;; WHEN: Sun Mar 12 13:31:20 CST 2023  
;; MSG SIZE rcvd: 55  
  
root@debian:~#
```

Por medio de la terminal de Debian de Linux, el putty de Windows así como la terminal de Windows, se comprueba la conectividad entre los equipos a través de la petición al nombre de estos mismos.

```
root@debian:~# ping Windows7.harosalazar.edu
PING Windows7.harosalazar.edu (192.168.40.131) 56(84) bytes of data.
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=1 ttl=128 time=0.977 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=2 ttl=128 time=1.10 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=3 ttl=128 time=1.13 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=4 ttl=128 time=0.899 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=5 ttl=128 time=1.26 ms
^C
--- Windows7.harosalazar.edu ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.899/1.073/1.259/0.125 ms
root@debian:~#
```

```
fernando@debian:~$ ping debian.harosalazar.edu
PING debian.harosalazar.edu (127.0.1.1) 56(84) bytes of data.
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=1 ttl=64 time=0.027 m
s
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=2 ttl=64 time=0.096 m
s
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=3 ttl=64 time=0.093 m
s
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=4 ttl=64 time=0.058 m
s
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=5 ttl=64 time=0.187 m
s
64 bytes from debian.harosalazar.edu (127.0.1.1): icmp_seq=6 ttl=64 time=0.081 m
s
^C
--- debian.harosalazar.edu ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5081ms
rtt min/avg/max/mdev = 0.027/0.090/0.187/0.049 ms
fernando@debian:~$ ping Windows7.harosalazar.edu
PING Windows7.harosalazar.edu (192.168.40.131) 56(84) bytes of data.
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=1 ttl=128 time=0.400 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=2 ttl=128 time=1.20 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=3 ttl=128 time=1.06 ms
64 bytes from Windows7.harosalazar.edu.40.168.192.in-addr.arpa (192.168.40.131):
  icmp_seq=4 ttl=128 time=1.05 ms
^C
--- Windows7.harosalazar.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```



```
Windows 7 x Debian 11.x 64-bit (4) x
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\usuario>ping debian.harosalazar.edu

Haciendo ping a debian.harosalazar.edu [192.168.40.133] con 32 bytes de datos:
Respuesta desde 192.168.40.133: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.40.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.40.133: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.40.133: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.40.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\usuario>ping Windows7.harosalazar.edu

Haciendo ping a Windows7.harosalazar.edu [192.168.40.131] con 32 bytes de datos:
Respuesta desde 192.168.40.131: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.40.131: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.40.131: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.40.131: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.40.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\usuario>_
```



## Conclusión

La actividad 4 se especializa en el desarrollo e instalación del servicio de DNS, es decir, el sistema de nombres de dominio, algo bastante similar a un directorio telefónico específicamente dentro del internet y por cómo se presentó en la explicación se puede ver como un sistema donde se relaciona un nombre de dominio con los datos como lo es la IP, propietario o seguridad, entre otros datos para identificar lo que se va a buscar, sin embargo, la práctica se centró principalmente en la explicación e instalación del servicio DNS dentro del servidor, más que comandos para el funcionamiento del DNS se vio como se instalaba por medio de comandos y a través de los archivos, los cuales se fueron modificando, ya sea para agregar las zonas directas o inversas para que la base de datos del DNS tenga la búsqueda a realizar, además de agregar el nombre de dominio, el cual era harosalazar.edu como anteriormente se había especificado, también se agregó el nombre de servidor como lo es debian y Windows, en adición, se añadieron las IP de las máquinas virtuales para que el servicio de DNS sea funcional esto dentro de archivos modificados, este servicio se puede comprobar ya sea en Linux o en Windows dentro de sus terminales, con el comando nslookup se pudo verificar la conexión con la máquina virtual y con la página a buscar, además se hicieron ping a estas máquinas virtuales utilizando el nombre de dominio con su servidor, de manera que se prueba la funcionalidad del protocolo DNS siendo el primer servicio instalado que se relaciona directamente con el dominio o nombre de páginas o máquinas que están fuera del alcance del usuario normal, lo cual añade una herramienta importante para el servidor que se está creando.