

SEGURIDAD INFORMÁTICA

PRÁCTICA 1 (PARTE II)

Alumno	Apellidos	Nombre	Curso
1	Garrido Cobo	Javier	4
2	Viñals Lage	Diego	4
3			

Los objetivos de esta segunda parte de la práctica 1 son los siguientes:

I. SERVICIO DNS

1. Estudiar el servicio DNS:
 - a. Proceso de resolución de nombres mediante el wireshark
 - b. Archivo de zona
 - c. Registros de recursos
2. Instalación y configuración en Linux del servidor DNS (BIND9)
3. Configuración del cliente DNS.
4. Instalación de un servidor Web en Linux
5. Conexión del cliente para acceder a la página web

Para ello instalaremos el servicio BIND9 y un servidor http en Linux (Apache o Nginx)

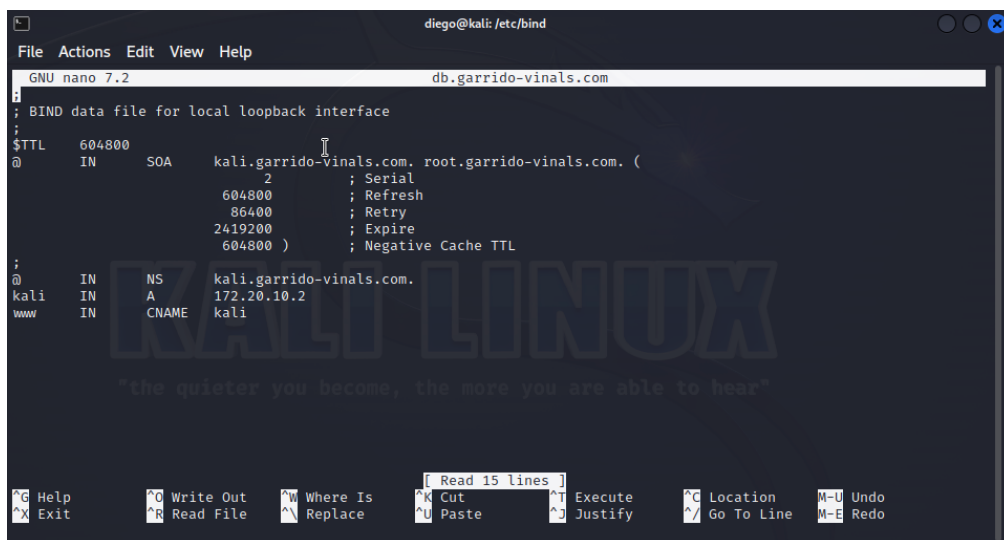
6. Investigar sobre los ataques que pueden sufrir este tipo de servidores

ACTIVIDADES

1. Instalar un servidor DNS en Linux y creación de una zona con el siguiente **nombre**: Nombre de la zona DNS: “los primeros apellidos de cada uno de los miembros del grupo separados por guion”.com.

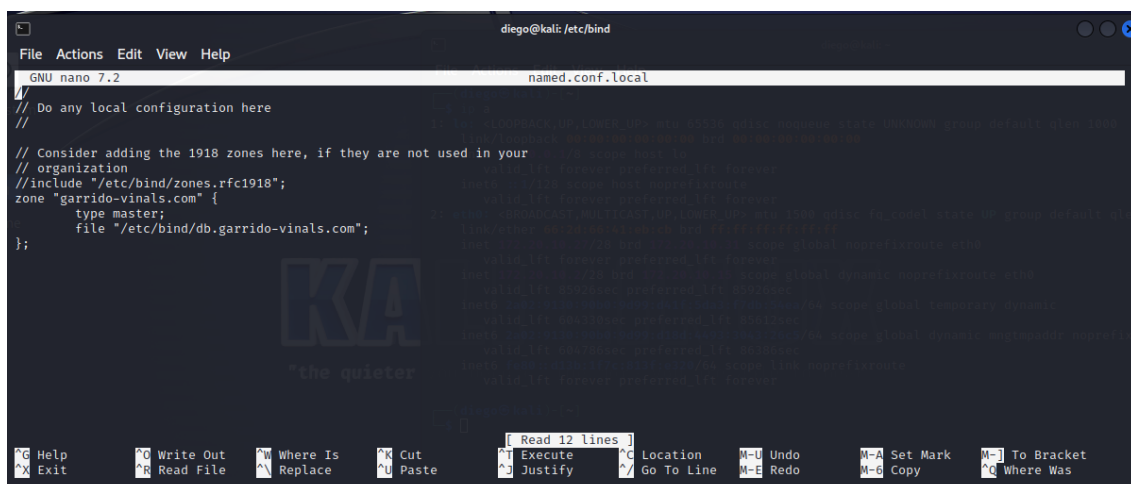
Ejemplo: si fuese mi apellido (Malagón) junto con alguien cuyo apellido fuese García el dominio sería: malagon-garcia.com

- a. ¿Cómo se instala y configura el servicio DNS?
 - i. Se instala mediante la orden **sudo apt-get install bind9**
 - ii. Configuración del archivo de zona



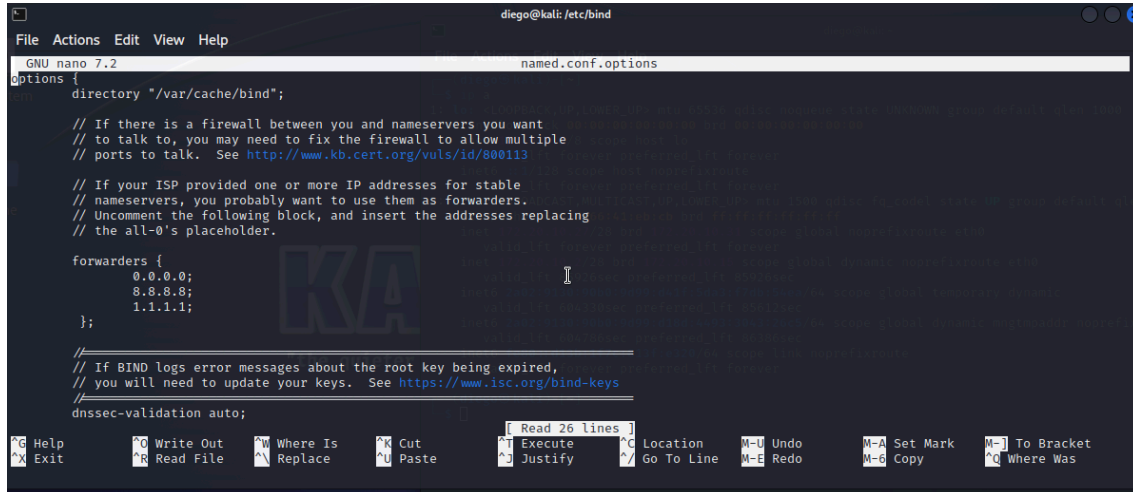
```
diego@kali: /etc/bind
GNU nano 7.2 db.garrido-vinals.com
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA kali.garrido-vinals.com. root.garrido-vinals.com. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS kali.garrido-vinals.com.
kali IN A 172.20.10.2
www IN CNAME kali
```

- iii. Se declara la zona en el fichero **named.conf.local**
- iv. Declaración de la zona y del fichero de zona



```
diego@kali: /etc/bind
GNU nano 7.2 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";
zone "garrido-vinals.com" {
    type master;
    file "/etc/bind/db.garrido-vinals.com";
};
```

- v. Se declaran los servidores DNS a los que se les pueden reenviar las peticiones (llamados forwarders). Para ello habrá que configurar nuestro servidor DNS para que reenvíe esta petición a cualquier otro servidor DNS (8.8.8.8 de Google o mejor el 1.1.1.1 de Cloudflare)



```
GNU nano 7.2 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

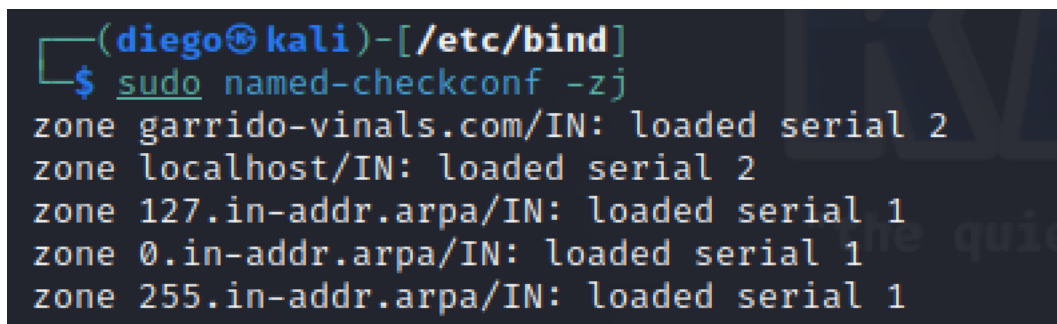
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        0.0.0.0;
        8.8.8.8;
        1.1.1.1;
    };

    // 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 auto;
}
```

- vi. Se reinicia el demonio con la orden **sudo service named restart**
- vii. Mediante la orden **named-checkconf -zj** comprueba que tu fichero de zona está bien definido.

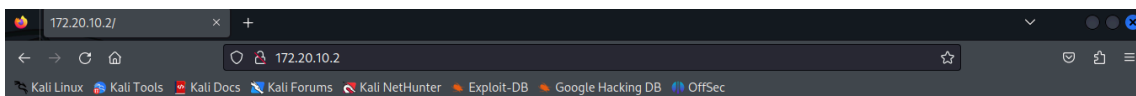


```
(diego@kali)-[/etc/bind]
$ sudo named-checkconf -zj
zone garrido-vinals.com/IN: loaded serial 2
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
```

2. Instalar un servidor Web en Linux (Nginx, Apache o cualquier otro) y publicar una página web de prueba en la que aparezca como mínimo el texto “Segunda parte de la práctica 1 y los nombres de los componentes del grupo”.

NOTA IMPORTANTE: En esta práctica el servidor DNS y el servidor web van a coincidir en el mismo equipo, pero en general esto no es así y el servidor DNS y el servidor web son equipos diferentes.

- a. ¿Cómo funciona y cómo se instala?
 - i. Se instala mediante la orden **sudo apt-get install apache2**
 - ii. Configuro mi sitio web y la página index en el directorio **/var/www/html/**
- b. Demuestra que el servidor apache está operativo
 - i. Puedo comprobar que funciona desde mi propio Linux accediendo desde el navegador a la dirección IP 127.0.0.1



Segunda parte de la practica 1

Los integrantes del grupo son: Diego Vinals y Javier Garrido

- ii. Mostrando evidencias de que el demonio está arrancado

```
(diego@kali)-[/var/www/html]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-10-17 17:04:17 CEST; 3min 32s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 106354 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 106364 (apache2)
       Tasks: 55 (limit: 2209)
      Memory: 24.0M
         CPU: 74ms
    CGroup: /system.slice/apache2.service
            └─106364 /usr/sbin/apache2 -k start
              106366 /usr/sbin/apache2 -k start
              106367 /usr/sbin/apache2 -k start
```

- iii. Mediante los comandos y las evidencias que el puerto del servicio HTTP está escuchando

```
(diego@kali)-[/var/www/html]
$ sudo ss -tlnl | grep 80
udp UNCONN 0 0 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
udp UNCONN 0 0 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
udp UNCONN 0 0 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
udp UNCONN 0 0 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
udp UNCONN 0 0 [fe80::d13b:1f7c:813f:e320]eth0:546 [::]:*
tcp LISTEN 0 10 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
tcp LISTEN 0 10 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
tcp LISTEN 0 10 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
tcp LISTEN 0 10 [fe80::d13b:1f7c:813f:e320]eth0:53 [::]:*
```

3. Comprobación del servidor DNS con nslookup

- a. Mediante la orden nslookup obtener la IP del servidor DNS predeterminado (escribiendo server). Esta IP debería ser la IP de nuestro Linux, que es el servidor DNS.

```
(diego@kali)-[/etc/bind]
$ nslookup
> server 172.20.10.2
Default server: 172.20.10.2
Address: 172.20.10.2#53
> server
Default server: 172.20.10.2
Address: 172.20.10.2#53
```

- b. Preguntar por www.malagon-garcia.com (en mi caso) y comprobar que nos devuelve la IP del servidor web (que en este caso es la misma que la del servidor DNS puesto que los dos servicios coinciden en el mismo equipo, pero como hemos dicho, no es lo habitual).

```
> www.garrido-vinals.com
;; communications error to 172.20.10.2#53 timed out
Server:      172.20.10.2
Address:     172.20.10.2#53

www.garrido-vinals.com canonical name = kali.garrido-vinals.com.
Name:   kali.garrido-vinals.com
Address: 172.20.10.2
```

- c. Siempre que carga la página WEB mediante la URL, ¿Se hace una consulta al DNS?

Si, cuando abres tu navegador y escribes una dirección web (como "www.ejemplo.com"), tu navegador no sabe automáticamente a qué servidor conectarse. Así que, para averiguarlo, hace una llamada a un directorio llamado DNS. Este directorio contiene todas las direcciones de sitios web y sus nombres fáciles de recordar, como "ejemplo.com." cada vez que visitas una página web, el navegador hace una llamada rápida al DNS para averiguar dónde debe ir.



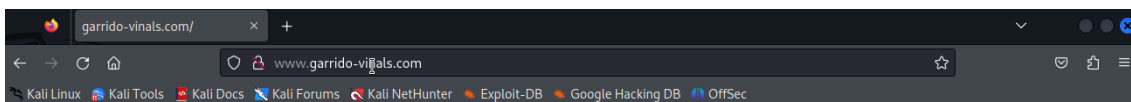
- d. **Resolución de una URL externa:** preguntar por www.twitter.com y comprobar que nos devuelve la IP del servidor web de Twitter.

```
> www.twitter.com
;; communications error to 172.20.10.2#53: timed out
Server:      172.20.10.2
Address:     172.20.10.2#53

Non-authoritative answer:
www.twitter.com canonical name = twitter.com.
Name:   twitter.com
Address: 104.244.42.65
```

4. **Conexión del cliente a un servidor web mediante la dirección:** <http://www.malagon-garcia.com> (ejemplo del nombre que he escrito antes; cada uno que ponga el suyo)

- a. Muestre el navegador del cliente con su URL donde se vea la página web con la URL donde aparezca el nombre del dominio creado.



Segunda parte de la practica 1

Los integrantes del grupo son: Diego Vinals y Javier Garrido

- b. ¿Qué diferencia hay entre poner la URL o poner la IP del servidor WEB en el navegador?

Usar una URL en lugar de una dirección IP en el navegador es más fácil para las personas, ya que las URLs son nombres de sitios web que recordamos fácilmente. Cuando usamos una URL, el navegador realiza una búsqueda para encontrar la dirección IP correspondiente al sitio web. Por otro lado, ingresar directamente una dirección IP es más técnico y menos amigable para los usuarios, ya que las direcciones IP son secuencias numéricas difíciles de recordar. Además, si cambias la dirección IP del servidor, los usuarios deben conocer la nueva IP, mientras que con una URL, los cambios pueden hacerse de manera más flexible y transparente para los usuarios.



- c. Si en el fichero de zona define la URL ftp.midominio.com (en su caso malagon-garcia.com, pero incluyendo la palabra ftp al principio) y lo asocia a la IP del servidor WEB, ¿qué sucede cuando escribe la URL ftp.midominio.com en el navegador?

Cuando defines en un archivo de zona la URL "ftp.midominio.com" y la asocia a la IP del servidor web, al escribir la URL "ftp.midominio.com" en el navegador, lo que sucede es que el navegador intentará acceder al servidor web utilizando el subdominio "ftp" como parte de la dirección. Esto significa que el navegador buscará la dirección IP del servidor web asociada con "ftp.midominio.com" y cargará el sitio web correspondiente.

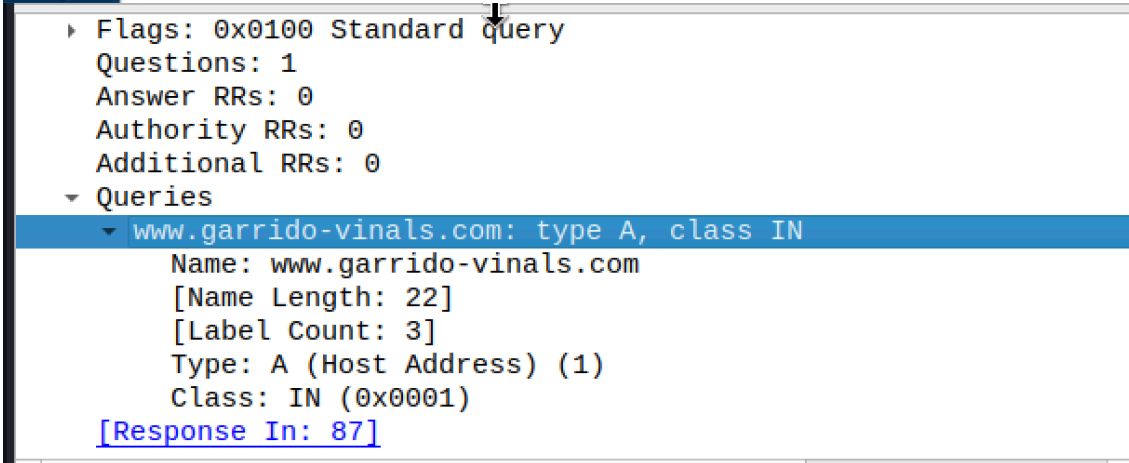
En otras palabras, la URL "ftp.midominio.com" dirige el navegador a buscar el servidor web al que está asociado el subdominio "ftp" dentro del dominio "midominio.com". Si la configuración DNS y del servidor web se ha realizado correctamente, se cargará el sitio web relacionado con "ftp.midominio.com" en el navegador. Esto permite tener múltiples subdominios en un dominio principal, cada uno apuntando a contenido o servicios específicos en el servidor web.

5. Uso de un sniffer como el Wireshark para:

- a. Identificar los paquetes que intervienen en la resolución de nombres entre el cliente y el servidor DNS mediante un ejemplo

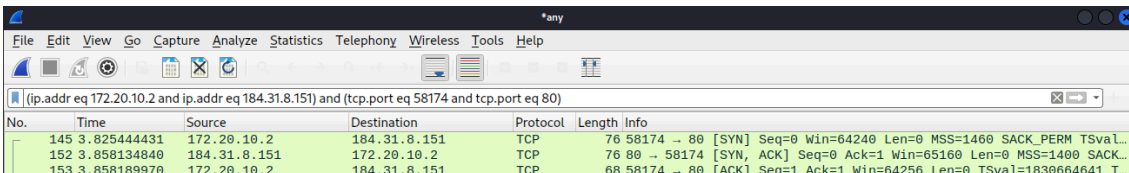
No.	Time	Source	Destination	Protocol	Length	Info
85	4.847217851	172.20.10.2	172.20.10.2	DNS	84	Standard query 0x1299 A www.garrido-vinals.com
86	4.847267309	172.20.10.2	172.20.10.2	DNS	84	Standard query 0xd09c AAAA www.garrido-vinals.com
87	4.847494476	172.20.10.2	172.20.10.2	DNS	119	Standard query response 0x1299 A www.garrido-vinals.com CNAME k...
88	4.847560101	172.20.10.2	172.20.10.2	DNS	144	Standard query response 0xd09c AAAA www.garrido-vinals.com CNAM...

- b. ¿Qué protocolo se utiliza en esta resolución? **UPD con puerto 53**
- c. ¿Qué tipo de registro es www? **Type A**



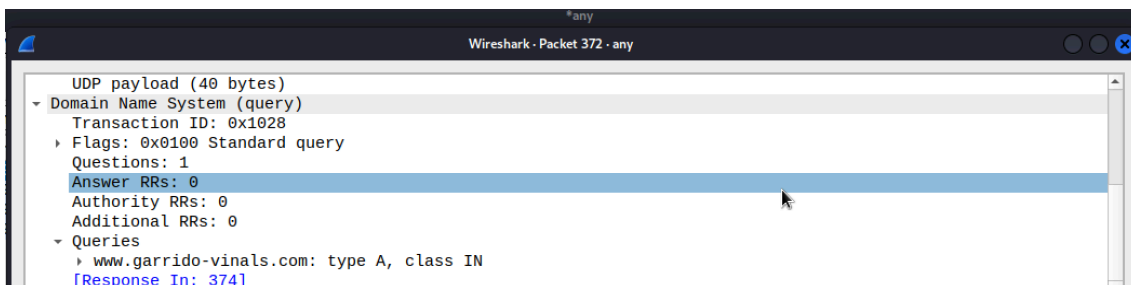
d. Identificar los paquetes que intervienen en la conexión cliente-servidor web:

i. Three-way handshake

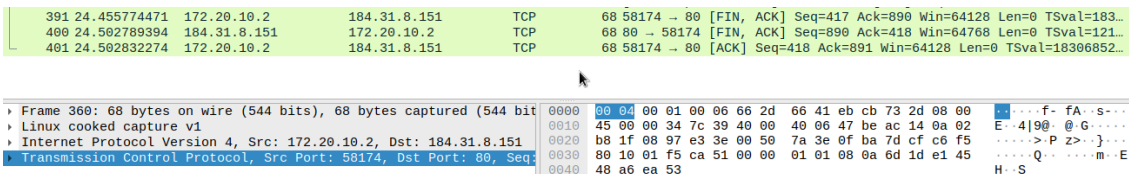


No.	Time	Source	Destination	Protocol	Length	Info
145	3.82544431	172.20.10.2	184.31.8.151	TCP	76	58174 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=...
152	3.858134840	184.31.8.151	172.20.10.2	TCP	76	80 → 58174 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1400 SACK=...
153	3.858189970	172.20.10.2	184.31.8.151	TCP	68	58174 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1830664641 T...

ii. Obtención de la página web



iii. Fin de conexión



No.	Time	Source	Destination	Protocol	Length	Info
391	24.455774471	172.20.10.2	184.31.8.151	TCP	68	58174 → 80 [FIN, ACK] Seq=417 Ack=890 Win=64128 Len=0 TSval=183...
400	24.502789394	184.31.8.151	172.20.10.2	TCP	68	80 → 58174 [FIN, ACK] Seq=890 Ack=418 Win=64768 Len=0 TSval=121...
401	24.502832274	172.20.10.2	184.31.8.151	TCP	68	58174 → 80 [ACK] Seq=418 Ack=891 Win=64128 Len=0 TSval=18306852...

Frame 360: 68 bytes on wire (544 bits), 68 bytes captured (544 bit)
 Linux cooked capture v1
 Internet Protocol Version 4, Src: 172.20.10.2, Dst: 184.31.8.151
 Transmission Control Protocol, Src Port: 58174, Dst Port: 80, Seq: 417, Len: 0

6. Parte de investigación

- a.** Investigar y contar brevemente en qué consisten los principales ataques que puede sufrir un servidor DNS. Explicar uno de ellos y buscar un ejemplo real de ataque sufrido por un servidor DNS junto con sus consecuencias

Existen varios tipos de ataque que puede sufrir un servidor DNS, el que vamos a explicar es el ataque de denegación de servicio.

Los atacantes llenan el servidor DNS con mucho volumen de tráfico falso, lo que sobrecarga el servidor y hace que no pueda responder a solicitudes reales.

En octubre de 2016, ocurrió un incidente real en el que un ataque DDoS masivo impactó al proveedor de servicios DNS llamado Dyn. Este ataque tuvo graves consecuencias, ya que provocó la caída de varios sitios web populares, entre ellos Twitter, Reddit, Spotify y Airbnb. Lo que hicieron los atacantes fue aprovechar una red de dispositivos de Internet de las cosas (IoT) que habían sido comprometidos previamente. Estos dispositivos, como cámaras de seguridad y enrutadores, se utilizaron para enviar una gran cantidad de tráfico de datos falso hacia los servidores DNS de Dyn. Esta avalancha de tráfico abrumador congestionó los servidores, lo que resultó en la interrupción del servicio para un gran número de usuarios de Internet. Este incidente ilustra la importancia de proteger los servidores DNS y estar preparados para defenderse contra ataques DDoS para garantizar el funcionamiento ininterrumpido de los servicios en línea. [1]

IMPORTANTE: Si se detecta que esta parte ha sido copiada la práctica será calificada con un 0.

Bibliografía

- [1] G. González, «Genbeta,» 27 Octubre 2016. [En línea]. Available: <https://www.genbeta.com/actualidad/el-ataque-contradyn-dns-que-sacudio-internet-fue-probablemente-obra-de-hackers-amateurs>. [Último acceso: 19 Octubre 2023].

INSTRUCCIONES

- Entrega:
 - Un archivo PDF a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.

- Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo (no hace falta volver a hacerlo si ya se ha hecho para la primera parte de la práctica). **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**

- El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.

- Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.

- **La fecha límite de entrega será el lunes 23 de octubre a las 23 horas.**

- No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.