

## **Introducción a las redes**

### **PRÁCTICA I (PARTE II)**

Los objetivos de esta primera parte de la práctica I 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.

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

```
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA  LnxMint-UnaiPuelles.katokii.com. root.katokii.com. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS   LnxMint-UnaiPuelles.katokii.com.
LnxMint-UnaiPuelles IN  A      10.1.206.105
www       IN      CNAME LnxMint-UnaiPuelles ; aqui iria el nombre del servidor web

@         IN      NS   localhost.
@         IN      A    127.0.0.1
@         IN      AAAA ::1
```

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

```
//
// 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 "katoki.com" {
    type master;
    file "/etc/bind/db.katoki.com";
};
```

- v. Se reinicia el demonio con la orden `sudo /etc/init.d/bind9 restart` o `sudo service bind9 restart`

**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 “Práctica I de Redes y los nombres de los componentes del grupo”**

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/index.html`

**3. Conexión del cliente a un servidor web mediante la dirección: <http://www.katokii.com> (ejemplo del nombre; cada uno que ponga el suyo)**



#### 4. 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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows two packets: a standard query (No. 2652) and a standard query response (No. 2653). The packet details pane for the selected packet (No. 2652) shows the following structure:

- Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.229
- User Datagram Protocol, Src Port: 63699, Dst Port: 53
- Domain Name System (query)
  - Standard query query 0xcdfd A www.katokii.com

The packet bytes pane shows the raw data in hexadecimal and ASCII format:

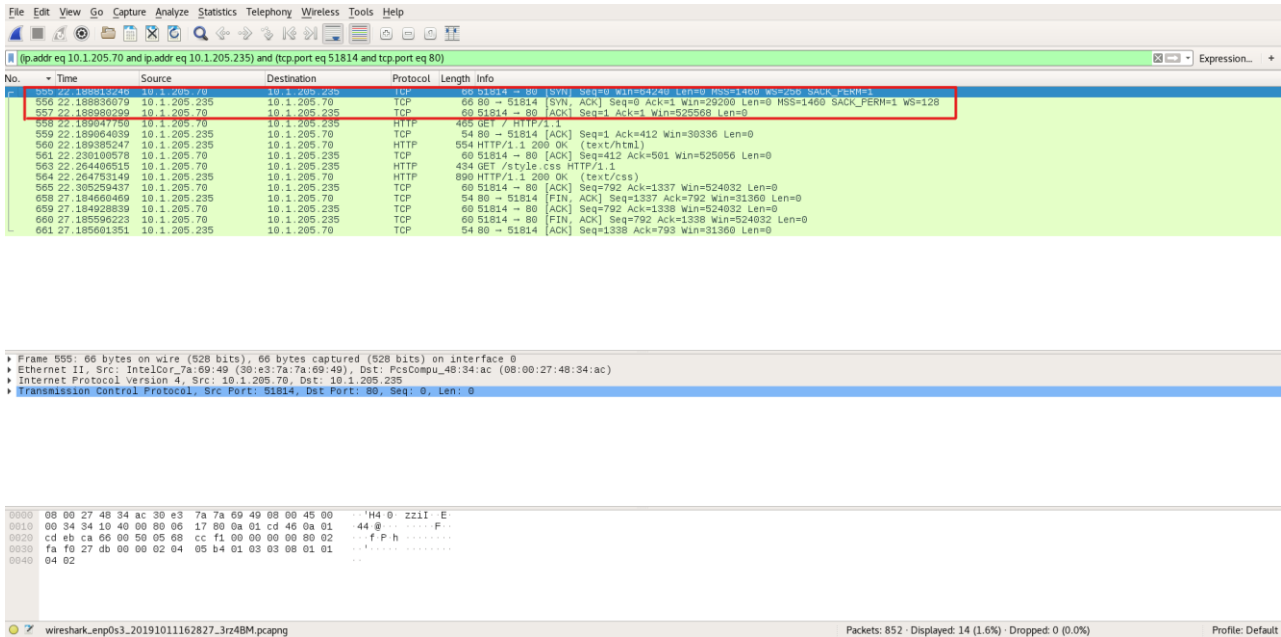
```

0000  00 00 27 3b 40 c2 30 e3 7a 7a 69 49 00 00 45 00  ...70-9-2211-E
0010  00 3d d2 0c 00 00 00 11 b9 75 8a 01 cd 46 8a 01  ...-U--F--
0020  cd e5 f8 d3 00 35 00 29 56 f3 cd fd 01 00 00 01  ...5-)V-----
0030  00 00 00 00 00 00 03 77 77 77 07 6b 61 74 6f 6b  ...www-katok
0040  69 69 03 63 6f 6d 00 00 01 00 01                ii.com-----
  
```

- b. ¿Qué protocolo se utiliza en esta resolución? Se utiliza el protocolo UDP
- c. ¿Qué tipo de registro es www? Es de tipo CNAME, es decir, es un alias de un equipo en concreto de ese dominio. Al servidor web se le asigna el alias www en vez de tener que poner el hostname del servidor.

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

i. Three-way handshake

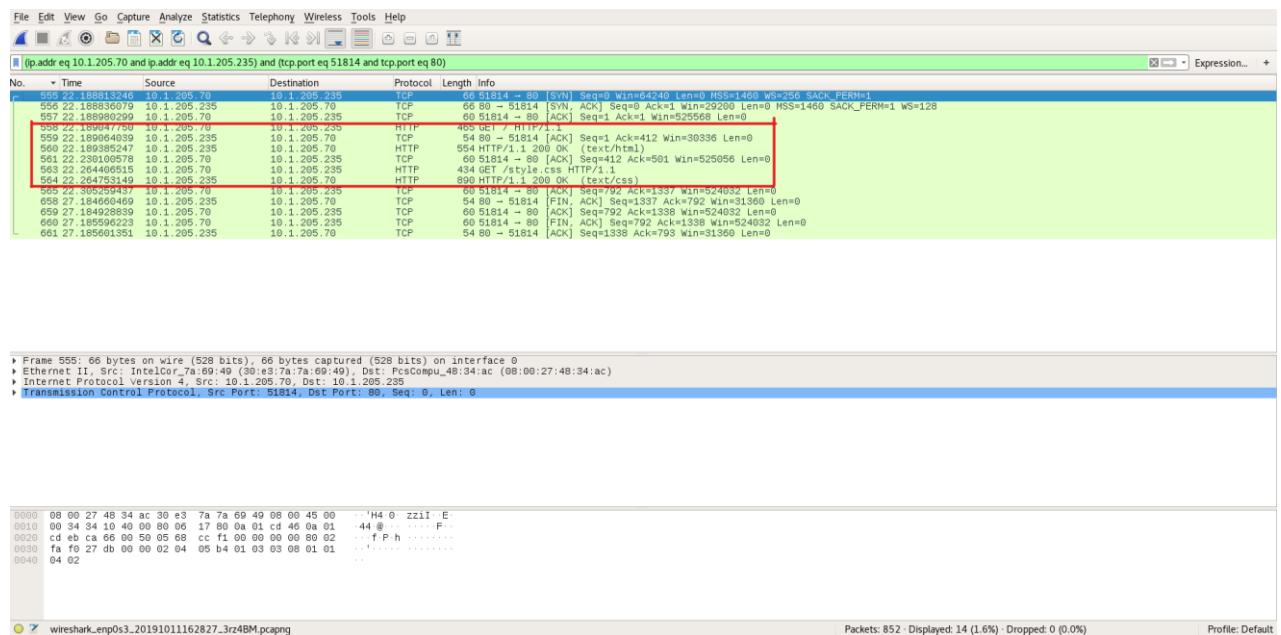


Frame 555: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 0, Len: 0

Frame 557: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 80, Dst Port: 51814, Seq: 1, Len: 0

Frame 559: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 1, Len: 0

ii. Obtención de la página web



Frame 555: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 0, Len: 0

Frame 557: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 80, Dst Port: 51814, Seq: 1, Len: 0

Frame 559: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 1, Len: 0

Frame 561: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 80, Dst Port: 51814, Seq: 1, Len: 0

Frame 563: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 1, Len: 0

### iii. Fin de conexión

Wireshark packet capture showing the end of a TCP connection. The packet list shows a sequence of packets from 555 to 661. Packets 659, 660, and 661 are highlighted in red, indicating the FIN sequence. The packet details pane shows the structure of packet 661: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
555	22.188813240	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
556	22.188836079	10.1.205.235	10.1.205.70	TCP	60	80 → 51814 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
557	22.188880299	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [ACK] Seq=1 Ack=1 Win=529568 Len=0
558	22.189047750	10.1.205.70	10.1.205.235	HTTP	465	GET / HTTP/1.1
559	22.189064039	10.1.205.235	10.1.205.70	TCP	54	80 → 51814 [ACK] Seq=1 Ack=412 Win=30336 Len=0
560	22.189395247	10.1.205.235	10.1.205.70	HTTP	554	HTTP/1.1 200 OK (text/html)
561	22.230100578	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [ACK] Seq=412 Ack=501 Win=525056 Len=0
563	22.264406515	10.1.205.70	10.1.205.235	HTTP	434	GET /style.css HTTP/1.1
564	22.264753140	10.1.205.235	10.1.205.70	HTTP	690	HTTP/1.1 200 OK (text/css)
565	22.305259437	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [ACK] Seq=792 Ack=1337 Win=524032 Len=0
559	27.184060469	10.1.205.235	10.1.205.70	TCP	54	80 → 51814 [FIN, ACK] Seq=1337 Ack=792 Win=31360 Len=0
659	27.184028539	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [ACK] Seq=792 Ack=1338 Win=524032 Len=0
660	27.185596223	10.1.205.70	10.1.205.235	TCP	60	51814 → 80 [FIN, ACK] Seq=792 Ack=1338 Win=524032 Len=0
661	27.185601351	10.1.205.235	10.1.205.70	TCP	54	80 → 51814 [ACK] Seq=1338 Ack=793 Win=31360 Len=0

Frame 555: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
 Ethernet II, Src: IntelCor\_7a:69:49 (30:e3:7a:7a:69:49), Dst: PcsCompu\_48:34:ac (08:00:27:48:34:ac)  
 Internet Protocol Version 4, Src: 10.1.205.70, Dst: 10.1.205.235  
 Transmission Control Protocol, Src Port: 51814, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 48 34 ac 30 e3 7a 7a 69 49 08 00 45 00 ...H4 0 zziI E  
 0010 00 34 34 10 40 00 00 06 17 00 0a 01 cd 46 0a 01 ...44 0 ...P  
 0020 cd eb ca 66 00 50 05 68 cc f1 00 00 00 00 80 02 ...f P h .....  
 0030 fa f0 27 db 00 00 02 04 05 b4 01 03 03 08 01 01 ...  
 0040 04 02

wireshark\_enp0s3\_20191011162827\_3rz4BM.pcapng Packets: 852 · Displayed: 14 (1.6%) · Dropped: 0 (0.0%) Profile: Default

## 5. 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.

Podemos encontrar varios ataques dns, entre ellos los más significativos son DNS Hijacking, Ataque DDoS, Tuneles DNS... entre otros.

DNS Hijacking consiste en alterar los servidores DNS del proveedor de Internet para que los usuarios accedan a servidores manejados por el atacante y conseguir información confidencial a través de la navegación del usuario. Por otro lado, el ataque DDoS, que es uno de los más comunes, consiste en saturar el servidor DNS con muchas conexiones hasta que el servidor se bloquea. Con esto lo que sucede es que los usuarios no pueden acceder a las páginas webs causando muchas pérdidas a las empresas.

### **Ataque real:**

Trabajadores del departamento de seguridad de Cisco en Talos revelaron el 18 de abril de 2019 que un grupo de hackers llamado "Sea Turtle" realizó una campaña de espionaje basada en secuestro DNS. El ataque afectó a 40 organizaciones. De este modo, tergiversaron múltiples dominios, llegando a afectar a proveedores de internet, objetivos militares y organizaciones gubernamentales entre otras víctimas.

Fuentes:

<https://securitytrails.com/blog/most-popular-types-dns-attacks>

<https://uss.com.ar/corporativo/tipos-ataques-dns-cuantos-existen-evitarlos/>

[https://www.schneier.com/blog/archives/2019/04/new\\_dns\\_hijacki.html](https://www.schneier.com/blog/archives/2019/04/new_dns_hijacki.html)

## 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 viernes 18 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.