

# Práctica Linux

Dns maestro/ esclavo / dnssec / apache options

17/11/2017

Athos Orío Choperena

# Practica dns maestro / esclavo / dnssec / directiva options apache

---

## Contenido

Escenario: .....	2
Parte 1: Configuración servidor dns maestro zona iescomercio.informatica.edu.....	2
Configuración de nombres de maquinas .....	3
Instalación de bind9 .....	4
Configuración de archivos necesarios:.....	5
Parte 2: Dns secundario .....	8
Parte 3: DnsSec.....	11
Parte 4: Apache directiva options: .....	20

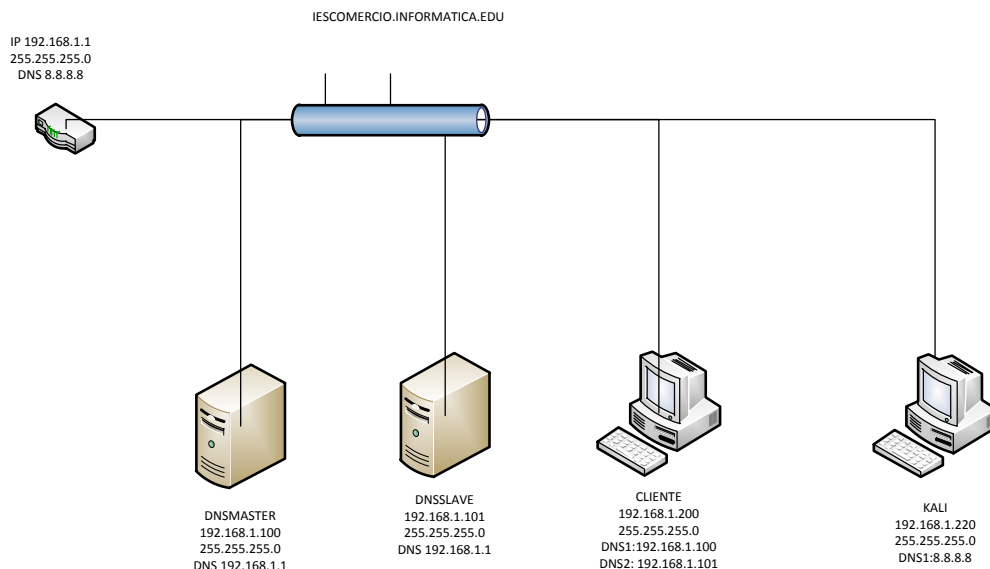
## Descripción general:

En este documento, se van a detallar los pasos para montar un servidor dns con bind para la zona iescomercio.informatica.edu, montaré también un servidor dns esclavo, que obtendrá la zona de la transferencia del servidor maestro. Finalmente, protegeremos la estructura con dnssec, que firma los datos que proceden del servidor dns, para que el “cliente” sepa con certeza que la información que solicitó procede efectivamente del servidor al que él cree que está preguntando.

Adicionalmente, haremos un estudio de la directiva options de apache, para ver que podemos hacer con ella.

## Escenario:

Tendremos dos servidores, uno será el servidor maestro y otro el esclavo, los dos correrán sistemas operativos Linux, en este caso usaremos Linux Mint, con la configuración de red que se detalla en el siguiente esquema. Dispondremos de un cliente en el que correrá Windows 7, y tendremos también una máquina Linux, que utilizaremos para realizar diferentes pruebas, esta máquina tendrá instalado kali Linux. Tendremos también un enrutador, que en este caso será un servidor Windows server 2016 con el rol de enrutador instalado, y con dos tarjetas de red, una en nat y otra en Lansegment con el resto de los equipos.



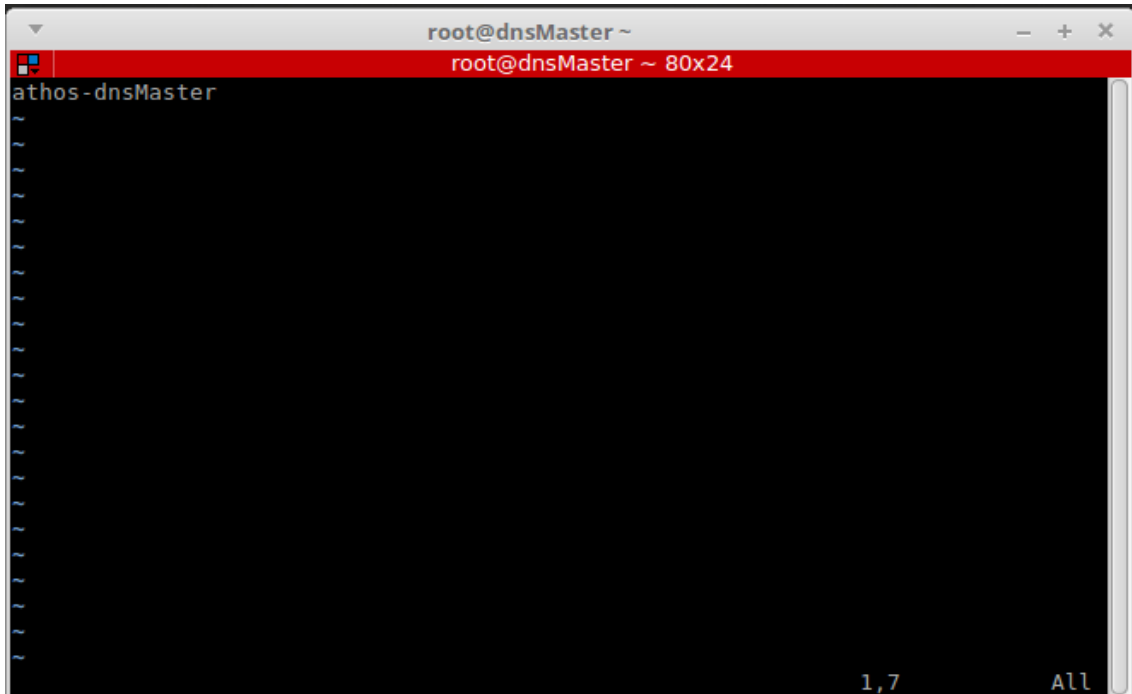
## Parte 1: Configuración servidor dns maestro zona iescomercio.informatica.edu

Partimos de un sistema limpio, con Linux mint instalado.

## Configuración de nombres de maquinas

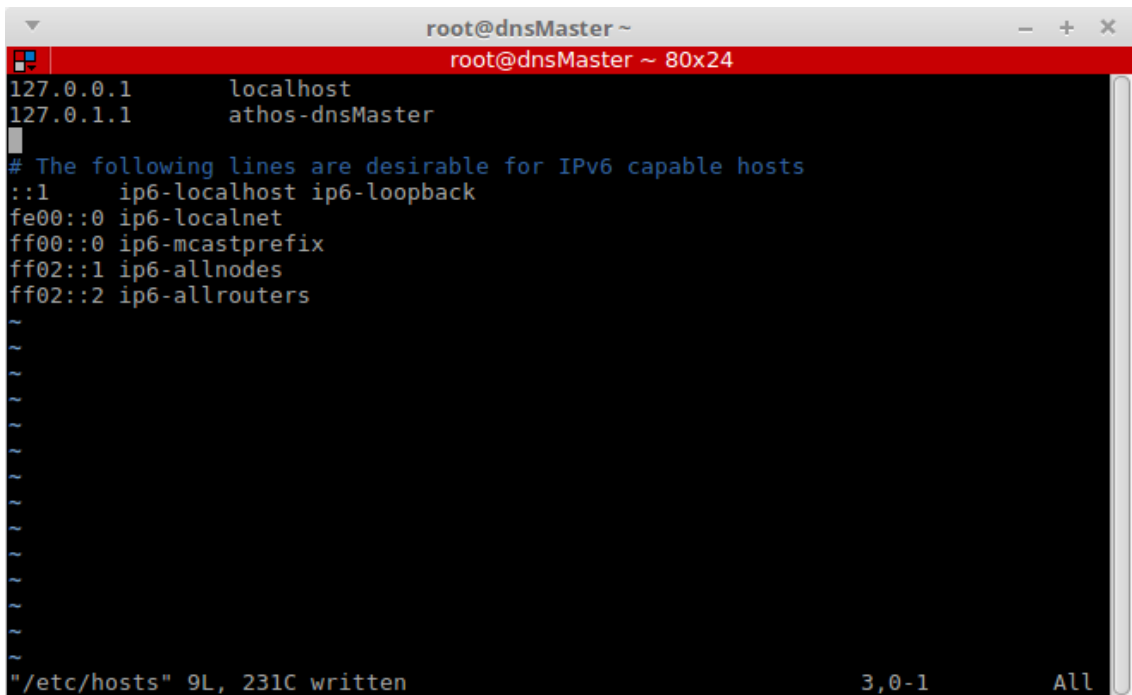
Lo primero que haremos es configurar las maquinas con los nombres que tendrán, el servidor maestro lo llamaremos athos-dnsMaster y el secundario athos-dnsSlave.

Para ellos, lo primero es modificar el archivo `/etc/hostname`



A terminal window titled 'root@dnsMaster ~' with a red header bar. The prompt is 'athos-dnsMaster'. The terminal shows a series of tilde characters '~' representing the contents of the file. At the bottom right, it indicates '1,7' lines and 'All' content.

Y también modificaremos el archivo `/etc/hosts`



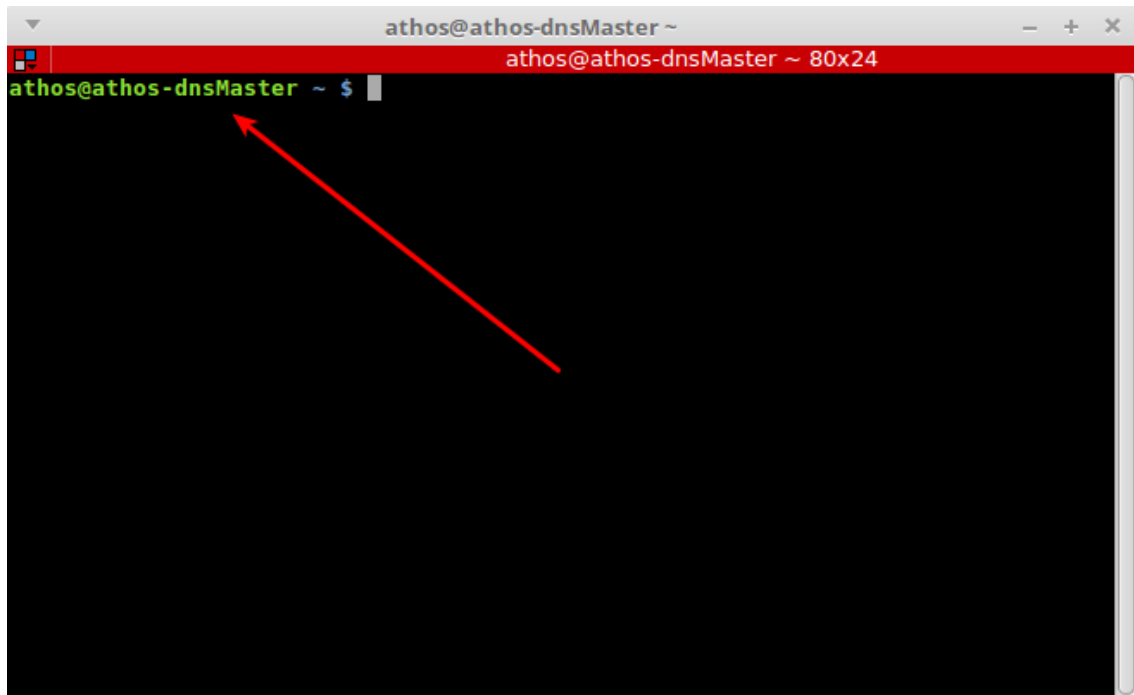
A terminal window titled 'root@dnsMaster ~' with a red header bar. The prompt is 'root@dnsMaster ~ 80x24'. The terminal shows the following content:

```
127.0.0.1    localhost
127.0.1.1    athos-dnsMaster

# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

At the bottom, it shows the file size and content count: `"/etc/hosts" 9L, 231C written`. At the bottom right, it indicates '3,0-1' lines and 'All' content.

Y nos quedará así



Repetiremos el proceso para el servidor secundario.

### Instalación de bind9

Instalaremos el servicio con aptitude install bind9

```

athos@athos-dnsMaster ~ $ sudo -s
[sudo] password for athos:
athos-dnsMaster ~ # aptitude install bind9
The following NEW packages will be installed:
  bind9 bind9utils{a} libirs141{a}
0 packages upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 591 kB of archives. After unpacking 2.954 kB will be used.
Do you want to continue? [Y/n/?] y
Get: 1 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 libirs141 amd64 1:9.10.3.dfsg.P4-8ubuntu1.8 [18,0 kB]
Get: 2 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 bind9utils amd64 1:9.10.3.dfsg.P4-8ubuntu1.8 [200 kB]
Get: 3 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 bind9 amd64 1:9.10.3.dfsg.P4-8ubuntu1.8 [372 kB]
Fetched 591 kB in 0s (1.480 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libirs141:amd64.
(Reading database ... 224528 files and directories currently installed.)
Preparing to unpack .../libirs141_1%3a9.10.3.dfsg.P4-8ubuntu1.8_amd64.deb ...
Unpacking libirs141:amd64 (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.10.3.dfsg.P4-8ubuntu1.8_amd64.deb ...
Unpacking bind9utils (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.10.3.dfsg.P4-8ubuntu1.8_amd64.deb ...
Unpacking bind9 (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
Setting up libirs141:amd64 (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Setting up bind9utils (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Setting up bind9 (1:9.10.3.dfsg.P4-8ubuntu1.8) ...
Adding group `bind' (GID 131) ...
Done.
Adding system user `bind' (UID 122) ...
Adding new user `bind' (UID 122) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
#
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...

athos-dnsMaster ~ # █

```

## Configuración de archivos necesarios:

Los archivos necesarios se encuentran en /etc/bind así que nos dirigiremos a ese directorio.

Lo primero que haremos es editar el archivo named.conf.local y añadiremos la zona. Tiene que quedar de la siguiente manera.

```

root@athos-dnsMaster /etc/bind
// 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 "iescomercio.informatica.edu." {
    type master;
    file "/etc/bind/iescomercio.informatica.edu.zone";
};

"named.conf.local" 13L, 273C written

```

Nos valdremos de los ejemplos para generar el archivo `iescomercio.informatica.edu.zone`, para esto, haremos una copia del archivo `db.empty`

```
athos-dnsMaster bind # cp db.empty iescomercio.informatica.edu.zone
athos-dnsMaster bind #
```

Y ahora editaremos el archivo, dejándolo de la siguiente manera:

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind 205x26

; BIND reverse data file for empty rfc1918 zone

;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$ORIGIN iescomercio.informatica.edu.
$TTL 86400
@ IN SOA iescomercio.informatica.edu. root.localhost. (
        1          ; Serial
        604800     ; Refresh
        86400     ; Retry
        2419200    ; Expire
        86400 )    ; Negative Cache TTL
;
@ IN NS localhost.
ns0 IN A 192.168.1.100
ns1 IN A 192.168.1.101
www IN A 192.168.1.102
ftp IN A 192.168.1.103
mail IN A 192.168.1.104
smtp IN A 192.168.1.105
nas IN A 192.168.1.106
;
;
-- INSERT --

```

Una vez hecho esto, reiniciaremos el servicio bind, y comprobaremos su funcionamiento

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind 205x26
athos-dnsMaster bind # /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
athos-dnsMaster bind # /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Sun 2017-10-29 18:31:39 CET; 3s ago
     Docs: man:named(8)
   Main PID: 3864 (named)
    CGroup: /system.slice/bind9.service
            └─3864 /usr/sbin/named -f -u bind

Oct 29 18:31:39 athos-dnsMaster named[3864]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 29 18:31:39 athos-dnsMaster named[3864]: zone localhost/IN: loaded serial 2
Oct 29 18:31:39 athos-dnsMaster named[3864]: zone iescomercio.informatica.edu/IN: loaded serial 1
Oct 29 18:31:39 athos-dnsMaster named[3864]: all zones loaded
Oct 29 18:31:39 athos-dnsMaster named[3864]: running
Oct 29 18:31:39 athos-dnsMaster named[3864]: zone iescomercio.informatica.edu/IN: sending notifies (serial 1)
Oct 29 18:31:39 athos-dnsMaster named[3864]: network unreachable resolving './DNSKEY/IN': 2001:500:84::b#53
Oct 29 18:31:39 athos-dnsMaster named[3864]: network unreachable resolving './NS/IN': 2001:500:84::b#53
Oct 29 18:31:39 athos-dnsMaster named[3864]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Oct 29 18:31:39 athos-dnsMaster named[3864]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
athos-dnsMaster bind #

```

Ahora comprobamos desde otra máquina que resuelve bien nuestras peticiones

```

root@athos:~# dig nas.iescomercio.informatica.edu @8.8.8.8

;<>> DiG 9.10.6-Debian <>> nas.iescomercio.informatica.edu @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 32622
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nas.iescomercio.informatica.edu. IN      A

;; AUTHORITY SECTION:
edu.                899      IN      SOA     a.edu-servers.net. nstld.verisign-grs.com. 1509298704 1800 900 604800 86400

;; Query time: 60 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Oct 29 18:38:46 CET 2017
;; MSG SIZE rcvd: 135

root@athos:~# dig nas.iescomercio.informatica.edu @192.168.1.100

;<>> DiG 9.10.6-Debian <>> nas.iescomercio.informatica.edu @192.168.1.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29405
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nas.iescomercio.informatica.edu. IN      A

;; ANSWER SECTION:
nas.iescomercio.informatica.edu. 86400 IN A      192.168.1.106

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS     localhost.

;; ADDITIONAL SECTION:
localhost.          604800 IN      A       127.0.0.1
localhost.          604800 IN      AAAA    ::1

;; Query time: 0 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Sun Oct 29 18:38:52 CET 2017
;; MSG SIZE rcvd: 143

root@athos:~#

```

Como vemos en la imagen anterior, si intentamos resolver nas.iescomercio.informatica.edu con el dns 8.8.8.8 no nos devuelve el registro tipo A, en cambio, solo resolvemos con nuestro servidor dns (192.168.1.100) si nos lo devuelve, diciéndonos que corresponde a la ip 192.168.1.106

Bien, esta parte, parece que funciona, ahora vamos a configurar el servidor esclavo.



## Parte 2: Dns secundario

Para ello, lo primero es instalar bind9 en el servidor secundario.

Seguidamente, vamos a configurar la zona en el servidor esclavo, el procedimiento es similar a lo que hicimos en el master, pero con alguna diferencia que detallaremos a continuación.

Editamos el archivo 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 "iescomercio.informatica.edu." {
    type slave;
    file "/var/lib/bind/iescomercio.informatica.edu.zone";
    masters { 192.168.1.100; };
};

"named.conf.local" 15L, 306C written

```

Como vemos, la estructura es similar pero con algunas diferencias.

Primero, el tipo, hemos puesto slave

La ruta del archivo es en /var/lib/bind en vez de en /etc/bind por temas de permisos de archivos.

En tercer lugar, hemos añadido la directiva masters, donde pondremos las direcciones ips de los servidores maestros.

Una vez hecho esto, salvaremos, y reiniciaremos el servicio.

```

root@athos-dnsSlave /etc/bind
root@athos-dnsSlave /etc/bind 205x26

athos-dnsSlave bind # /etc/init.d/bind9 restart
[ OK ] Restarting bind9 (via systemctl): bind9.service.
athos-dnsSlave bind # /etc/init.d/bind9 status
bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Drop-In: /run/systemd/generator/bind9.service.d
        50-sserv.conf-$named.conf
Active: active (running) since Sun 2017-10-29 18:51:31 CET; 3s ago
Docs: man:named(8)
Main PID: 3728 (named)
CGroup: /system.slice/bind9.service
        └─3728 /usr/sbin/named -f -u bind

Oct 29 18:51:31 athos-dnsSlave named[3728]: network unreachable resolving 'C.RDUT-SERVERS.NET/AAAA/IN': 2001:503:ba3e::2:30#53
Oct 29 18:51:31 athos-dnsSlave named[3728]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Oct 29 18:51:31 athos-dnsSlave named[3728]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Oct 29 18:51:31 athos-dnsSlave named[3728]: transfer of 'iescomercio.informatica.edu/IN' from 192.168.1.100#53: connected using 192.168.1.101#48521
Oct 29 18:51:31 athos-dnsSlave named[3728]: zone iescomercio.informatica.edu/IN: transferred serial 1
Oct 29 18:51:31 athos-dnsSlave named[3728]: zone iescomercio.informatica.edu/IN: transfer started
Oct 29 18:51:31 athos-dnsSlave named[3728]: transfer of 'iescomercio.informatica.edu/IN' from 192.168.1.100#53: Transfer status: success
Oct 29 18:51:31 athos-dnsSlave named[3728]: transfer of 'iescomercio.informatica.edu/IN' from 192.168.1.100#53: Transfer completed: 1 messages, 10 records, 287 bytes, 0.001 secs (287000 bytes/sec)
Oct 29 18:51:31 athos-dnsSlave named[3728]: zone iescomercio.informatica.edu/IN: sending notifies (serial 1)
Oct 29 18:51:31 athos-dnsSlave named[3728]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0da#3
athos-dnsSlave bind # ls /var/lib/bind/
bind9-default.md5sum iescomercio.informatica.edu.zone
athos-dnsSlave bind #

```

Como vemos en la imagen anterior, se nos ha creado el fichero de zona. Si inspeccionamos su contenido, vemos que está en algún formato en el que no podemos ver su contenido de forma correcta.

[illegible]

Llegados aquí, el siguiente paso es configurar las notificaciones de cambios del servidor maestro a los esclavos, para ello, vamos a editar la zona que hemos creado anteriormente y vamos a añadir la directiva notify yes. Lo haremos en el archivo `/etc/bind/named.conf.local`

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind 205x45
//
// 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 "iescomercio.informatica.edu." {
    type master;
    file "/etc/bind/iescomercio.informatica.edu.zone";
    notify yes;
    //also-notify { 192.168.1.101; };
    allow-transfer { 192.168.1.101; };
};

```

Como se ve en la imagen, hemos añadido la directiva `notify yes`. Esto lo que hará, es enviar notificaciones de los cambios cuando el serial de la zona haya incrementado, y lo hará solo a los servidores dns que tengan un registro en esta zona. Si los servidores dns esclavos no tendrían un registro NS deberíamos utilizar la directiva `also-notify { ip; }`, pero en este caso, vamos a añadir estos registros para hacerlo correctamente.

Para ello vamos a nuestro fichero de zona, y añadimos los registros correspondientes como se muestra en la imagen.

```

root@athos-dnsMaster /etc/bind
BIND reverse data file for empty rfc1918 zone

DO NOT EDIT THIS FILE - it is used for multiple zones.
Instead, copy it, edit named.conf, and use that copy.

$ORIGIN iescomercio.informatica.edu.
$TTL 86400
@ IN SOA iescomercio.informatica.edu. root.localhost. (
    5556 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    86400 ) ; Negative Cache TTL

@ IN NS localhost.
ns0 IN A 192.168.1.100
@ IN NS ns0
ns1 IN A 192.168.1.101
@ IN NS ns1
www IN A 192.168.1.102
ftp IN A 192.168.1.103
mail IN A 192.168.1.104
smtp IN A 192.168.1.105
nas IN A 192.168.1.106

```

Ahora, vamos a comprobar si esto funciona correctamente. Desde la maquina kali, vamos a hacer una solicitud del registro soa, y lo vamos a hacer al servidor secundario, y marcándole

que no queremos que haga la búsqueda de forma recursiva (esto lo haremos añadiendo al comando dig el parámetro +norecurs)

Vamos a hacer la consulta:

```

root@athos: ~
root@athos: ~ 235x52
root@athos:~# dig SOA iescomercio.informatica.edu @192.168.1.101 +norecurs

; <<>> DiG 9.10.6-Debian <<>> SOA iescomercio.informatica.edu @192.168.1.101 +norecurs
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3199
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;iescomercio.informatica.edu. IN SOA

;; ANSWER SECTION:
iescomercio.informatica.edu. 86400 IN SOA iescomercio.informatica.edu. root.localhost. 5556 604800 86400 2419200 86400

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS localhost.

;; ADDITIONAL SECTION:
ns0.iescomercio.informatica.edu. 86400 IN A 192.168.1.100
ns1.iescomercio.informatica.edu. 86400 IN A 192.168.1.101
localhost. 604800 IN A 127.0.0.1
localhost. 604800 IN AAAA ::1

;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Sun Oct 29 19:15:13 CET 2017
;; MSG SIZE rcvd: 232

root@athos:~#

```

Ahora, vamos a editar el archivo de nuestra zona, aumentando el serial y volveremos a hacer la consulta. Paralelamente a esto, vamos a poner a capturar con wireshark para ver si podemos localizar el paquete de la notificación.

Como se ve en la siguiente imagen, y sin meternos a fondo en wireshark vemos que el maestro (192.168.1.100) envía un paquete de notificación de cambio de zona, a lo que le sigue una petición del esclavo (192.168.1.101) de transferencia de zona.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.1.101	DNS	137	Zone change notification 0x7f4b SOA iescomercio.informatica.edu SOA iescomercio.informatica.edu
2	0.000192409	192.168.1.101	192.168.1.100	DNS	98	Standard query response 0x724f SOA iescomercio.informatica.edu OPT
3	0.000285989	192.168.1.101	192.168.1.100	DNS	274	Standard query response 0x724f SOA iescomercio.informatica.edu NS ns1.iescomercio.informatica.edu NS localhost NS ns0...
4	0.000699539	192.168.1.100	192.168.1.101	TCP	74	45189 -> 53 [SYN] Seq=614030808 Len=0 MSS=1460 SACK_PERM=1 TSval=451891 TSecn=0 W=128
5	0.000702872	192.168.1.101	192.168.1.100	TCP	74	53 -> 45189 [SYN, ACK] Seq=614030808 Len=0 MSS=1460 SACK_PERM=1 TSval=567625 TSecn=452811 W=128
6	0.000949846	192.168.1.100	192.168.1.101	DNS	163	Standard query 0x5296 IXFR iescomercio.informatica.edu SOA iescomercio.informatica.edu
7	0.001059554	192.168.1.101	192.168.1.100	TCP	66	45189 -> 53 [ACK] Seq=614030808 Win=29112 Len=0 TSval=452811 TSecn=567625
8	0.001156855	192.168.1.100	192.168.1.101	TCP	66	53 -> 45189 [ACK] Seq=614030808 Win=29112 Len=0 TSval=567625 TSecn=452811
9	0.001268093	192.168.1.100	192.168.1.101	DNS	393	Standard query response 0x5296 IXFR iescomercio.informatica.edu SOA iescomercio.informatica.edu NS ns0.iescomercio.informatica.edu NS ns1.iescomercio...
10	0.001305533	192.168.1.101	192.168.1.100	TCP	66	45189 -> 53 [ACK] Seq=614030808 Win=29112 Len=0 TSval=452811 TSecn=567625
11	0.001305533	192.168.1.101	192.168.1.100	TCP	66	45189 -> 53 [ACK] Seq=614030808 Win=29112 Len=0 TSval=452811 TSecn=567625
12	0.001564739	192.168.1.100	192.168.1.101	DNS	137	Zone change notification 0x5795 SOA iescomercio.informatica.edu SOA iescomercio.informatica.edu
13	0.001707797	192.168.1.101	192.168.1.100	TCP	66	53 -> 45189 [ACK] Seq=614030808 Win=29112 Len=0 TSval=567625 TSecn=452811
14	0.001738826	192.168.1.100	192.168.1.101	TCP	66	45189 -> 53 [ACK] Seq=614030808 Win=29112 Len=0 TSval=567625 TSecn=452811
15	0.001738826	192.168.1.101	192.168.1.100	TCP	66	45189 -> 53 [ACK] Seq=614030808 Win=29112 Len=0 TSval=567625 TSecn=452811
16	0.001977799	192.168.1.100	192.168.1.101	DNS	87	Zone change notification response 0x5795 SOA iescomercio.informatica.edu
17	0.518635328	192.168.1.101	158.227.96.15	NTP	90	NTP Version 4, client
18	0.553018843	158.227.96.15	192.168.1.101	NTP	90	NTP Version 4, server

Si desde la maquina kali volvemos a hacer la petición del soa del esclavo de forma no recursiva, vemos lo siguiente.

```

root@athos:~# dig SOA iescomercio.informatica.edu @192.168.1.101 +norecurs
; <<> DiG 9.10.6-Debian <<> SOA iescomercio.informatica.edu @192.168.1.101 +norecurs
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 24547
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;iescomercio.informatica.edu. IN SOA
;; ANSWER SECTION:
iescomercio.informatica.edu. 86400 IN SOA iescomercio.informatica.edu. root.localhost 5559 604800 86400 2419200 86400
;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS localhost.
;; ADDITIONAL SECTION:
ns0.iescomercio.informatica.edu. 86400 IN A 192.168.1.100
ns1.iescomercio.informatica.edu. 86400 IN A 192.168.1.101
localhost. 604800 IN A 127.0.0.1
localhost. 604800 IN AAAA ::1
;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Sun Oct 29 19:22:53 CET 2017
;; MSG SIZE rcvd: 232
root@athos:~#

```

Lo que quiere decir que en esta petición, la zona ha sido actualizada con respecto a la anterior petición.

Bien, hasta aquí, todo funciona de forma correcta.

### Parte 3: DnsSec

Ahora, vamos a implementar dnssec, pero... ¿Qué es DNSSEC?

El protocolo DNSSEC es una extensión del propio protocolo DNS aumentando su seguridad. Gracias a DNSSEC los clientes podrán obtener autenticación del origen de datos DNS, además también permite la integridad de estos datos haciendo que no se pueda modificar sin que lo sepamos.

Más información en <https://www.redeszone.net/2015/12/27/que-es-dnssec-y-como-comprobamos-si-el-dominio-de-la-web-que-visitas-lo-soporta/>

Lo primero que tenemos que hacer es activar dnssec en el fichero de opciones named.conf.options y añadiremos las siguientes directivas

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind
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
    //=====
    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
~
~

```

Ahora, tenemos que crear dos certificados, uno para firmar la zona, y otro para la clave

Para ello, ejecutaremos un par de comandos para que se generen dichos pares de claves, pero primero, vamos a instalar haveged, que es una utilidad que acelera la generación de las claves, no es imprescindible, pero hará que las claves se generen en unos segundos en vez de tardar más.

Una vez instalado haveged, ejecutamos el siguiente comando para generar el certificado de zona. (previamente iremos al directorio /var/cache/bind)

```

root@athos-dnsMaster /var/cache/bind
root@athos-dnsMaster /var/cache/bind 205x40
athos-dnsMaster bind # pwd
/var/cache/bind
athos-dnsMaster bind # aptitude install haveged
The following NEW packages will be installed:
  haveged libhaveged1
0 packages upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 49,8 kB of archives. After unpacking 196 kB will be used.
Do you want to continue? [Y/n/?] y
Get: 1 http://archive.ubuntu.com/ubuntu xenial/universe amd64 libhaveged1 amd64 1.9.1-3 [21,8 kB]
Get: 2 http://archive.ubuntu.com/ubuntu xenial/universe amd64 haveged amd64 1.9.1-3 [28,0 kB]
Fetched 49,8 kB in 10s (4,738 B/s)
Selecting previously unselected package libhaveged1:amd64.
(Reading database ... 224643 files and directories currently installed.)
Preparing to unpack .../libhaveged1.9.1-3_amd64.deb ...
Unpacking libhaveged1:amd64 (1.9.1-3) ...
Selecting previously unselected package haveged.
Preparing to unpack .../haveged.1.9.1-3_amd64.deb ...
Unpacking haveged (1.9.1-3) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
Setting up libhaveged1:amd64 (1.9.1-3) ...
Setting up haveged (1.9.1-3) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
athos-dnsMaster bind # dnssec-keygen -a NSEC3RSASHA1 -b 2048 -n ZONE iescomercio.informatica.edu
Generating key pair.....+++ .....+++
Kiescomercio.informatica.edu.+007+57155
athos-dnsMaster bind # dnssec-keygen -f KSK -a NSEC3RSASHA1 -b 4096 -n ZONE iescomercio.informatica.edu
Generating key pair.....+++ .....+++
Kiescomercio.informatica.edu.+007+23835
athos-dnsMaster bind #

```

Esto nos habrá generado 4 archivos

```

athos-dnsMaster bind # ls -l
total 24
-rw-r--r-- 1 root root 983 Oct 29 20:01 Kiescomercio.informatica.edu.+007+23835.key
-rw----- 1 root root 3319 Oct 29 20:01 Kiescomercio.informatica.edu.+007+23835.private
-rw-r--r-- 1 root root 638 Oct 29 20:01 Kiescomercio.informatica.edu.+007+57155.key
-rw----- 1 root root 1779 Oct 29 20:01 Kiescomercio.informatica.edu.+007+57155.private
-rw-r--r-- 1 bind bind 1421 Oct 29 19:53 managed-keys.bind
-rw-r--r-- 1 bind bind 512 Oct 29 19:53 managed-keys.bind.jnl
athos-dnsMaster bind #

```

Ahora, vamos a añadir las claves a nuestra zona, esto lo podemos hacer de forma manual editando el archivo de zona, o también lo podemos hacer con un bucle como se ve en la siguiente imagen.

```

root@athos-dnsMaster /var/cache/bind
root@athos-dnsMaster /var/cache/bind 205x40
athos-dnsMaster bind # for key in $(ls Kiescomercio.informatica.edu*.key); do echo "${INCLUDE $key}" >> /etc/bind/iescomercio.informatica.edu.zone; done
athos-dnsMaster bind # cat /etc/bind
bind/
bind/ bindresvport.blacklist
athos-dnsMaster bind # cat /etc/bind/iescomercio.informatica.edu.zone
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$ORIGIN iescomercio.informatica.edu.
$TTL 86400
@ IN SOA iescomercio.informatica.edu. root.localhost. (
    5563      ; Serial
    604800    ; Refresh
    86400     ; Retry
    2419200   ; Expire
    86400 )   ; Negative Cache TTL
;
@ IN NS localhost.
ns0 IN A 192.168.1.100
@ IN NS ns0
ns1 IN A 192.168.1.101
@ IN NS ns1
www IN A 192.168.1.102
ftp IN A 192.168.1.103
mail IN A 192.168.1.104
smtp IN A 192.168.1.105
nas IN A 192.168.1.106
$INCLUDE Kiescomercio.informatica.edu.+007+23835.key
$INCLUDE Kiescomercio.informatica.edu.+007+57155.key
athos-dnsMaster bind #

```

Lo siguiente es firmar la zona, para esto se hace con el siguiente comando:

```

root@athos-dnsMaster /var/cache/bind
root@athos-dnsMaster /var/cache/bind 205x40
athos-dnsMaster bind # dnsssec-signzone -A -3 $(head -c 1000 /dev/random | shasum | cut -b 1-16) -N INCREMENT -o iescomercio.informatica.edu -t /etc/bind/iescomercio.informatica.edu.zone
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
Algorithm: NSEC3RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 1 active, 0 stand-by, 0 revoked
/etc/bind/iescomercio.informatica.edu.zone.signed
Signatures generated: 20
Signatures retained: 0
Signatures dropped: 0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Signing time in seconds: 0.020
Signatures per second: 963.205
Runtime in seconds: 0.023
athos-dnsMaster bind #

```

Este comando, nos ha generado el archivo iescomercio.informatica.zone.signed que es igual que el original solo que firmado.

```
athos-dnsMaster bind # ls -l
total 72
-rw-r--r-- 1 root root 3954 Sep 15 17:20 bind.keys
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.0
-rw-r--r-- 1 root root 271 Sep 15 17:20 db.127
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.255
-rw-r--r-- 1 root root 353 Sep 15 17:20 db.empty
-rw-r--r-- 1 root root 270 Sep 15 17:20 db.local
-rw-r--r-- 1 root root 3171 Sep 15 17:20 db.root
-rw-r--r-- 1 root bind 703 Oct 29 20:05 iescomercio.informatica.edu.zone
-rw-r--r-- 1 root bind 14081 Oct 29 20:07 iescomercio.informatica.edu.zone.signed
-rw-r--r-- 1 root bind 463 Sep 15 17:20 named.conf
-rw-r--r-- 1 root bind 490 Sep 15 17:20 named.conf.default-zones
-rw-r--r-- 1 root bind 359 Oct 29 19:27 named.conf.local
-rw-r--r-- 1 root bind 933 Oct 29 20:00 named.conf.options
-rw-r----- 1 bind bind 77 Oct 29 18:21 rndc.key
-rw-r--r-- 1 root root 1317 Sep 15 17:20 zones.rfc1918
athos-dnsMaster bind #
```

Si miramos el contenido del archivo, vemos que ha añadido al archivo original los campos RRSIG

```
athos-dnsMaster bind # cat iescomercio.informatica.edu.zone.signed
; File written on Sun Oct 29 20:07:54 2017
; dnssec signzone version 9.10.3-P4-Ubuntu
iescomercio.informatica.edu. 86400 IN SOA iescomercio.informatica.edu. root.localhost. (
    5564      ; serial
    604800    ; refresh (1 week)
    86400     ; retry (1 day)
    2419200   ; expire (4 weeks)
    86400     ; minimum (1 day)
)
    86400    RRSIG    SOA 7 3 86400 (
        20171128180754 20171029180754 57155 iescomercio.informatica.edu.
        sRLU/HfzguiZnRqPFRcSHX+1GusVabeaNw6p
        j1ncge4c8lMCVJ549VMYxZzZ0gNfgDdtJmz3
        Ne0I9uvGG0/EIWh9it8ZbTJBM+LB92/0UaU
        r2G6+9a6oJexk6i9jH4AYzg5q2rfVdixWZwt
        tRwqmvpuL7esj2iPYDLruvpb6nWrK8mCd8p0
        CT657W9/gHbaesot3A4Boezli04ivbKxVvyQ
        BV7Q/pladaE0ofK7ucv3dajrxm8204R9dzXL
        nBv4zCueJ5FmboY0cX8GlnySwlcilf1nLEqL
        WPcuXDSwcDVEaMLzaGe/9bTsFsWqX6kVUYQD
        UDC1FcITUcpEd5q08g== )
    86400    NS       ns0.iescomercio.informatica.edu.
    86400    NS       ns1.iescomercio.informatica.edu.
    86400    NS       localhost.
    86400    RRSIG    NS 7 3 86400 (
        20171128180754 20171029180754 57155 iescomercio.informatica.edu.
        rYJ0gIaxBZvmV0gFWcmGYa0kXEp5hxuhCR1
        q7elg6yqtlvMRrdHWR+NiXsZoP2wK2nRoloC
        p78R9IcPp+B78suDHJzdWcsgHpVv07XxANC6
        UCRWrPNZzPSDF/sRWRhvdhcrDb7IXouKDpuW
        7Iyk4ZRLaL/YVZOeh0Exh4BniXdiBlfWE8nW
        10aXvNlf4P+axBzPm2wLgxGLy0qf9qWAW4UW
        j0yDnRtCZa7g9H1cLpVLcwGp9ma0rs/FXSH
        b/Msv4q5n3jd6FW0UkzPe5ciIU0DGo1JVAj
        X9LGBKb5onRWE+ObKcC+QcM0YfpPknGxSvUN
        4Hfa8EvG051+TYDKyg== )
    86400    DNSKEY   256 3 7 (
        AwEAAb48SLr71XcUjKUvyXYFXpEIz6tiCxtT
        c5+GXGHkg18AtB6/8Eb0XqbcAbpKmaJwkcN2
        WN2713T+g+XsF5MAKm8chw6G50kRBZCtLVMD
        d5cm19/whFbEcZkd3K7c9WKEcbJd7bE5FEiT
        1+QczsmhMddQ1UmpRX9L4wX44ogoC0eSzhnR
        h18muuoSaAfujS4FGregPxx8LfY1xlkGIdTL
        VeEdHx9WBULKP0byIudojLcIsG/jPori6YL3
        AS50n4ql71ZAhzdAdSph9MD4+mrX8H62p16d
        FGMv2Cfi8VF5y0oayYBh/iwIUDKzxX92kdFj
        US40SD9PldhC2Q96tnXLP4s=
        ) ; ZSK; alg = NSEC3RSASHA1; key id = 57155
    86400    DNSKEY   257 3 7 (
        AwEAAZc31EZeQLKTxkG4VGf0NzGjziDxNvP/
        rS/T/tI9AE+M10AGD9Wiim4UM0B7IlpuAe9L
        UHiUnjEcdE2vvvxGTZXHttz/EcNB6VsNVKdA
```

Ahora en nuestro archivo /etc/bind/named.conf.local, tendremos que decirle que coja el archivo firmado en vez del original.

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind 205x54
//
// 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 "iescomercio.informatica.edu." {
    type master;
    file "/etc/bind/iescomercio.informatica.edu.zone.signed";
    notify yes;
    //also-notify { 192.168.1.101; };
    allow-transfer { 192.168.1.101; };
};

```

Ahora, salvaremos y reiniciaremos bind.

```

athos-dnsMaster bind # /etc/init.d/bind9 restart && /etc/init.d/bind9 status
[ ok ] Restarting bind9 (via systemctl): bind9.service.
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Sun 2017-10-29 20:13:49 CET; 59ms ago
     Docs: man:named(8)
   Process: 5272 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
  Main PID: 5277 (named)
    CGroup: /system.slice/bind9.service
            └─5277 /usr/sbin/named -f -u bind

Oct 29 20:13:49 athos-dnsMaster named[5277]: configuring command channel from '/etc/bind/rndc.key'
Oct 29 20:13:49 athos-dnsMaster named[5277]: command channel listening on ::1#953
Oct 29 20:13:49 athos-dnsMaster named[5277]: managed-keys-zone: loaded serial 39
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone iescomercio.informatica.edu/IN: loaded serial 5564 (DNSSEC signed)
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone localhost/IN: loaded serial 2
Oct 29 20:13:49 athos-dnsMaster named[5277]: all zones loaded
Oct 29 20:13:49 athos-dnsMaster named[5277]: running
Oct 29 20:13:49 athos-dnsMaster named[5277]: zone iescomercio.informatica.edu/IN: sending notifies (serial 5564)
athos-dnsMaster bind #

```

Vamos a hacer la comprobación desde la maquina kali

Primero comprobamos dnskey



```

root@athos: ~
root@athos:~# dig DNSKEY iescomercio.informatica.edu @192.168.1.100 +multiline

;<>> DiG 9.10.3-P4-Debian <>> DNSKEY iescomercio.informatica.edu @192.168.1.100 +multiline
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 34264
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;iescomercio.informatica.edu. IN      DNSKEY

;; ANSWER SECTION:
iescomercio.informatica.edu. 86400 IN DNSKEY 257 3 7 (
    AwEAAZc3IEZeQLKTxkG4VGfONzGjzIdXNvP/rS/T/tI9
    AE+Ml0AGD9W1im4UM0B7ItpuAe9LUH1UnjEcdE2vVvXG
    TZxHttz/EcNB6VsNVKdAPotpzIBUXWth4isL00pRnFz
    0GLB4axmvnf1SjpvTu8T5bYfDrMajRdkKEULNTY07+5
    TM9YzfZBcFm0j340MZTQwtXIBthkX5i6cr1cbsgTxxII
    uTK4H09auYJ7R/8Vc6S7gvxA6wEn9jsNUZg0M6YpRveU
    1/AC0wG01j9MMu08H7+/LEJSqk6yDQCQ0Ct92vkZB9W2
    h0F/AJPb9GbedumXaZd18UjUhn3LqrrxAWY93qWhYkxy7
    GdsTz/7ZAE+9vu9I7LDoicA1/0Q2XgcUN3c06r/ITro
    Jo8KzIdZQhLQMpXfQeQXyz6V5q4u07Z12Sv033vkhR
    eq56pW/b47VLarAGAkd3gt1WfGmHZ6EeF1m1gjTMQv6
    +vmW0Ltu0A1ZjofIjxqhp0jbu2FpPT5W1H5AHEtDoBm
    nE82/kyVXI09o4qMesPqXjJnthF9PZKSYNoHqr/P2V10
    Bj+YZ+mpzjW3+0qtrCHms9IKv06ykrBG2HfjbVU3p+b
    37ma89oLTZ9Rq5uGmtwB7v4z/V8M03F+mZ3BnmNUZGb
    J+IfN1bSv65jDsMXkAULuXP1zR67
    ) ; KSK; alg = NSEC3RSASHA1; key id = 23835
iescomercio.informatica.edu. 86400 IN DNSKEY 256 3 7 (
    AwEAAb48SLr71XcUjKuvyYFXpEIz6t1CxttC5+GXGHk
    g18AtB6/8Eb0XqbcAbpKmaJwkCN2WN2713T+g+XsF5MA
    Km8chw6G50kR8ZCtLVMDd5cm19/whFbEcZkD3K7c9WKE
    cbJd7bE5FE1t1+0czsmHdd01Umprx9L4wX44ogoC0eS
    zhnR18muuoSaAfusj4FGregPxx8LfY1x1kG1dTLVeEd
    Hx9WBULKP0byIudojLcIsG/fPor16YL3AS5Qn4qL71ZA
    hzdAdSph9MD4+mrX8H62p16dFGMv2CFI8VF5Y0oayYBh
    /iWlUDKzxX02k0fJUS405D9PlahC2096tnX1P4s=
    ) ; ZSK; alg = NSEC3RSASHA1; key id = 57155

;; Query time: 0 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Sun Oct 29 20:20:17 CET 2017
;; MSG SIZE rcvd: 864

root@athos:~#

```

También podemos consultar un registro tipo A

```

root@athos:~# dig A nas.iescomercio.informatica.edu @192.168.1.100 +multiline +dnssec +noadditional

;<>> DiG 9.10.3-P4-Debian <>> A nas.iescomercio.informatica.edu @192.168.1.100 +multiline +dnssec +noadditional
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 31866
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nas.iescomercio.informatica.edu. IN A

;; ANSWER SECTION:
nas.iescomercio.informatica.edu. 86400 IN A 192.168.1.106
nas.iescomercio.informatica.edu. 86400 IN RRSIG A 7 4 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    J7naQv13M0p/KmZ+na0u5Zky78E/F77a10Ev61Xw68
    A4eTVR2p300z/rXBn9IV00Ujs8V99co08U1l+M8BSKY
    60wVQ0PUCoCXrf08tzKwL9t8yHkc8LrfJHud1Zxh0g
    jNv9PY1bHHYXpHV/SowgujJhAaAytjdNf8zdQUMMAhf
    yKac5AK9x4zJebvDYGL6002KA6RnalR6ozKs2XtuoYMA
    /Auk99cN06TD0zj1NNRH1qbW05W2LbGTzC9ZPMBA9w04
    LAL705PzDLLxd3kuLdU2j/0ltlyD78A+WHO+JE8FPF0U
    DIX9J68uzCGW0lmNDVQMTk/GbUgPHANIQ== )

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS localhost.
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN RRSIG NS 7 3 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    rY30gIaxB2vmV0gFWcmGMYa0KXepShuXCR1q7e1g6vq
    t1vMRrdHwR+N1XgZ0P2wK2nRoLoCp78R9ICp+B78suD
    H3zdWcSgHpVV07XxANC6UCRrPNZ7PSDF/sRwRbVdhcr
    Db7IXouK0puw77Iyk4ZRLal/VYVZ0eh0Exh48n1Xd1B1fW
    E8nW1QaXvNLf4P+axBzPm2wLgXGLy0gF9qWAW4UWj0yD
    nRtCZa7g9H1cLpVLcwgGp9ma0rs/FXSHb/Msv4q5n3cj
    d6FW0UkzPeSc1IU0DGoLJVAjX9LGBKbSonRWE+0bKcC+
    QcM8YfpKnGxSvuN4Hfa8EvG051+TYDKyg== )

;; Query time: 0 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Sun Oct 29 20:22:15 CET 2017
;; MSG SIZE rcvd: 1471

root@athos:~#

```

Ahora, vamos a hacer una consulta al servidor esclavo, para ver si nos devuelve los datos firmados, y si solicita las transferencias de zona

```

Applications Places System
root@athos: ~
root@athos: ~ 235x52

;<<< Dig 9.10.3-P4-Debian <<< SOA iescomercio.informatica.edu @192.168.1.101 +multiline +dnssec +noadditional +norecurs
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 3019
;; flags: qr aa ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
iescomercio.informatica.edu. IN SOA

;; ANSWER SECTION:
iescomercio.informatica.edu. 86400 IN SOA iescomercio.informatica.edu. root.localhost. (
    5564      ; serial
    604800    ; refresh (1 week)
    86400     ; retry (1 day)
    2419200   ; expire (4 weeks)
    86400     ; minimum (1 day)
)
iescomercio.informatica.edu. 86400 IN RRSIG SOA 7 3 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    sRLU/HfzguiznRqPFRc3HX+1GusVabeaW6pJlncge4c
    81MCVJ549VMYxZz20gNfgDdtJmz3Ne0I9uvG60/EIWhh
    91t8ZbTJBM+LB92/0UaUr2G6+9a6oJexk619JH4AYzg5
    q2rfVdixWZwttRwqmvPUL7esj2iPYDLruvpb6nWrK8mC
    dBpOCT657W9/gHbaesot3A4BoezLi041vbKxVvQ8V7Q
    /pLadaE0ofK7uCV3dajrxm82Q4R9dzXlnBv4zcUeJ5Fm
    boY0cX8GlnySwlcilfInLqLwPcuXDSwcDVEaMLzaGe/
    9bTsFsWqX6KvUYQUDUClFclTUCpEd5q08g== )

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS localhost.
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN RRSIG NS 7 3 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    rYJ0gIaxBZvmV0gFWcmGMYa0KXEp5hxxuhCR1q7elg6yq
    t1vMRrdHWR+N1XsZp2K2nRoloCp78R9IcPp+B78suD
    HJzdwKcsgHpVV07XxANC6UCRWRPNZzP5DF/sRwRnVdhcr
    Db7IXouKdpUw7Iyk4ZRLaL/YVZ0eh0Exh4BniXdiB1fW
    E8nwiQaXvNlf4P+axBzPm2wLgxGLy0qf9qWAW4UWj0yD
    nRtCZa7g9H1cLpLVcwgG9ma0rs/FXSHb/Msv4q5n3cj
    d6FM0UkzPe5c1IU00GoLJVAjX9LGBkb5onRwE+0bkKc+
    QcM0YfPknGxSvulN4Hfa8EvG051+TYDKyg== )

;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Sun Oct 29 20:23:14 CET 2017
;; MSG SIZE rcvd: 1492

root@athos:~#

```

Actualizamos el serial del archivo signed de zona y vemos lo siguiente

```

root@athos: ~
root@athos: ~ 235x52

;<<< Dig 9.10.3-P4-Debian <<< SOA iescomercio.informatica.edu @192.168.1.101 +multiline +dnssec +noadditional +norecurs
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 23913
;; flags: qr aa ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
iescomercio.informatica.edu. IN SOA

;; ANSWER SECTION:
iescomercio.informatica.edu. 86400 IN SOA iescomercio.informatica.edu. root.localhost. (
    5570      ; serial
    604800    ; refresh (1 week)
    86400     ; retry (1 day)
    2419200   ; expire (4 weeks)
    86400     ; minimum (1 day)
)
iescomercio.informatica.edu. 86400 IN RRSIG SOA 7 3 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    sRLU/HfzguiznRqPFRc3HX+1GusVabeaW6pJlncge4c
    81MCVJ549VMYxZz20gNfgDdtJmz3Ne0I9uvG60/EIWhh
    91t8ZbTJBM+LB92/0UaUr2G6+9a6oJexk619JH4AYzg5
    q2rfVdixWZwttRwqmvPUL7esj2iPYDLruvpb6nWrK8mC
    dBpOCT657W9/gHbaesot3A4BoezLi041vbKxVvQ8V7Q
    /pLadaE0ofK7uCV3dajrxm82Q4R9dzXlnBv4zcUeJ5Fm
    boY0cX8GlnySwlcilfInLqLwPcuXDSwcDVEaMLzaGe/
    9bTsFsWqX6KvUYQUDUClFclTUCpEd5q08g== )

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS localhost.
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN RRSIG NS 7 3 86400 (
    20171128180754 20171029180754 57155 iescomercio.informatica.edu.
    rYJ0gIaxBZvmV0gFWcmGMYa0KXEp5hxxuhCR1q7elg6yq
    t1vMRrdHWR+N1XsZp2K2nRoloCp78R9IcPp+B78suD
    HJzdwKcsgHpVV07XxANC6UCRWRPNZzP5DF/sRwRnVdhcr
    Db7IXouKdpUw7Iyk4ZRLaL/YVZ0eh0Exh4BniXdiB1fW
    E8nwiQaXvNlf4P+axBzPm2wLgxGLy0qf9qWAW4UWj0yD
    nRtCZa7g9H1cLpLVcwgG9ma0rs/FXSHb/Msv4q5n3cj
    d6FM0UkzPe5c1IU00GoLJVAjX9LGBkb5onRwE+0bkKc+
    QcM0YfPknGxSvulN4Hfa8EvG051+TYDKyg== )

;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Sun Oct 29 20:27:25 CET 2017
;; MSG SIZE rcvd: 1492

root@athos:~#

```

Es decir, sí que se realiza transferencia de zona, pero tenemos un problema, que si queremos añadir un nuevo registro por ejemplo tipo A tenemos que cambiar el fichero sin firmar, y volver a firmarlo.

Así, que primero añadimos el registro, y procedemos a firmar el archivo

```

root@athos-dnsMaster /etc/bind
root@athos-dnsMaster /etc/bind 205x54
BIND reverse data file for empty rfc1918 zone
DO NOT EDIT THIS FILE - it is used for multiple zones.
Instead, copy it, edit named.conf, and use that copy.
$ORIGIN iescomercio.informatica.edu.
$TTL 86400
IN SOA iescomercio.informatica.edu. root.localhost. (
    5571      ; Serial
    604800    ; Refresh
    86400     ; Retry
    2419200   ; Expire
    86400 )   ; Negative Cache TTL
;
IN NS localhost.
ns0 IN A 192.168.1.100
ns1 IN A 192.168.1.101
www IN A 192.168.1.102
ftp IN A 192.168.1.103
mail IN A 192.168.1.104
smtp IN A 192.168.1.105
nas IN A 192.168.1.106
impression IN A 192.168.1.107
$INCLUDE iescomercio.informatica.edu.+007+23835.key
$INCLUDE iescomercio.informatica.edu.+007+57155.key

```

Después iremos al directorio donde tenemos los certificados, y crearemos un pequeño script, que lo que hará, es firmar nuestro archivo de zona, y generara a partir de ahí el archivo de zona firmado, reiniciara el bind, y nos mostrara es estado. El script es el siguiente.

```

root@athos-dnsMaster /var/cache/bind
root@athos-dnsMaster /var/cache/bind 205x22
dassec-signzone -A -3 $(head -c 1000 /dev/random | shasum | cut -b 1-16) -N INCREMENT -o iescomercio.informatica.edu -t /etc/bind/iescomercio.informatica.edu.zone
/etc/init.d/bind restart && /etc/init.d/bind status

```

Ahora vamos a comprobar la hora del archivo iescomercio.informatica.edu.zone.signed

```

athos-dnsMaster bind # ls -l /etc/bind
total 72
-rw-r--r-- 1 root root 3954 Sep 15 17:20 bind.keys
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.0
-rw-r--r-- 1 root root 271 Sep 15 17:20 db.127
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.255
-rw-r--r-- 1 root root 353 Sep 15 17:20 db.empty
-rw-r--r-- 1 root root 270 Sep 15 17:20 db.local
-rw-r--r-- 1 root root 3171 Sep 15 17:20 db.root
-rw-r--r-- 1 root bind 732 Oct 29 20:31 iescomercio.informatica.edu.zone
-rw-r--r-- 1 root bind 15315 Oct 29 20:50 iescomercio.informatica.edu.zone.signed
-rw-r--r-- 1 root bind 463 Sep 15 17:20 named.conf
-rw-r--r-- 1 root bind 490 Sep 15 17:20 named.conf.default-zones
-rw-r--r-- 1 root bind 364 Oct 29 20:13 named.conf.local
-rw-r--r-- 1 root bind 933 Oct 29 20:00 named.conf.options
-rw-r--r-- 1 bind bind 77 Oct 29 18:21 rndc.key
-rw-r--r-- 1 root root 1317 Sep 15 17:20 zones.rfc1918

```

Ejecutamos nuestro script

```

athos-dnsMaster bind # sh firmar.iescomercio.informatica.edu.zone.sh
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
Algorithm: NSEC3RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                ZSKs: 1 active, 0 stand-by, 0 revoked
/etc/bind/iescomercio.informatica.edu.zone.signed
Signatures generated: 22
Signatures retained: 0
Signatures dropped: 0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Signing time in seconds: 0.020
Signatures per second: 1055.611
Runtime in seconds: 0.025
[ ok ] Restarting bind9 (via systemctl): bind9.service.
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
  Drop-In: /run/systemd/generator/bind9.service.d
           └─50-insserv.conf-$named.conf
   Active: active (running) since Sun 2017-10-29 20:52:28 CET; 49ms ago
     Docs: man:named(8)
  Process: 6168 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
    Main PID: 6173 (named)
      CGroup: /system.slice/bind9.service
              └─6173 /usr/sbin/named -f -u bind

Oct 29 20:52:28 athos-dnsMaster named[6173]: command channel listening on 127.0.0.1#953
Oct 29 20:52:28 athos-dnsMaster named[6173]: configuring command channel from '/etc/bind/rndc.key'
Oct 29 20:52:28 athos-dnsMaster named[6173]: command channel listening on ::1#953
Oct 29 20:52:28 athos-dnsMaster named[6173]: managed-keys-zone: journal file is out of date: removing journal file
Oct 29 20:52:28 athos-dnsMaster named[6173]: managed-keys-zone: loaded serial 47
Oct 29 20:52:28 athos-dnsMaster named[6173]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 29 20:52:28 athos-dnsMaster named[6173]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 29 20:52:28 athos-dnsMaster named[6173]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 29 20:52:28 athos-dnsMaster named[6173]: zone localhost/IN: loaded serial 2
Oct 29 20:52:28 athos-dnsMaster named[6173]: zone iescomercio.informatica.edu/IN: loaded serial 5572 (DNSSEC signed)

```

Y volvemos a mirar la fecha del archivo

```

athos-dnsMaster bind # ls -l /etc/bind
total 72
-rw-r--r-- 1 root root 3954 Sep 15 17:20 bind.keys
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.0
-rw-r--r-- 1 root root 271 Sep 15 17:20 db.127
-rw-r--r-- 1 root root 237 Sep 15 17:20 db.255
-rw-r--r-- 1 root root 353 Sep 15 17:20 db.empty
-rw-r--r-- 1 root root 270 Sep 15 17:20 db.local
-rw-r--r-- 1 root root 3171 Sep 15 17:20 db.root
-rw-r--r-- 1 root bind 732 Oct 29 20:31 iescomercio.informatica.edu.zone
-rw-r--r-- 1 root bind 15315 Oct 29 20:52 iescomercio.informatica.edu.zone.signed
-rw-r--r-- 1 root bind 463 Sep 15 17:20 named.conf
-rw-r--r-- 1 root bind 490 Sep 15 17:20 named.conf.default-zones
-rw-r--r-- 1 root bind 364 Oct 29 20:13 named.conf.local
-rw-r--r-- 1 root bind 933 Oct 29 20:00 named.conf.options
-rw-r--r-- 1 bind bind 77 Oct 29 18:21 rndc.key
-rw-r--r-- 1 root root 1317 Sep 15 17:20 zones.rfc1918
athos-dnsMaster bind #

```

Como vemos, se ha actualizado, ahora comprobamos desde la maquina kali el nuevo registro que añadimos

```

root@athos:~# dig A impresion.iescomercio.informatica.edu @192.168.1.101 +multiline +dnssec +noadditional +norecurs
; <<> DIG 9.10.3-P4-Debian <<> A impresion.iescomercio.informatica.edu @192.168.1.101 +multiline +dnssec +noadditional +norecurs
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 12302
;; flags: qr aa ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
; impresion.iescomercio.informatica.edu. IN A

;; ANSWER SECTION:
impresion.iescomercio.informatica.edu. 86400 IN A 192.168.1.107
impresion.iescomercio.informatica.edu. 86400 IN RRSIG A 7 4 86400 (
    20171128184749 20171029184749 57155 iescomercio.informatica.edu.
    IHLw8LWYPIUaz0F/c4ZdJk47SD7H44j8u7n52MgsTRnx
    CVcup2+sEkHkESX0sNfC93jDnMTnlGkXJ+U4Wku7G0S
    xHS4qkmFLjG0N9a0Cg10uGcAt/TsDmWyll+dmqAF7/YE
    ijkcmkWKgrC6RaoY5Bf6MRjFgFA9ERLjlvhCXeLzhEBt
    d5qgKsFtBy/tqB01N+pCZzHBFbX+RVZCtSd8Wye0qfGc
    1EVAjKpT9HcEmXCBJT+xU4s6vkyoPDcvmF8mECyf7dVY
    WbcGJTCxshjByWha41Tn9zqoB9mHoVpINsqex6luSUS
    ZLmgCt0oLCCLLPY2YpJfD5aqpNPyoxiYQ== )

;; AUTHORITY SECTION:
iescomercio.informatica.edu. 86400 IN NS ns0.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS ns1.iescomercio.informatica.edu.
iescomercio.informatica.edu. 86400 IN NS localhost.
iescomercio.informatica.edu. 86400 IN RRSIG NS 7 3 86400 (
    20171128184749 20171029184749 57155 iescomercio.informatica.edu.
    qJo3t03lcW6aQRr+UeUbPuzwXehBygZD7jyzsblupwGf
    dxGy/PVes7dIp0zNKMcUz7dHrxnsLxL3wInKut1r5Nh
    7P3KXpXF3Xt6K2bICLhMpG02BRg5L1yqSPchZwsTD4L
    RkZ0qtixRxoXWQ4S0+8NM+0Aj2WxP3/7x/50uLc6eTju
    o//FxFjuxDvpuShxu1emm/M89BURR9mDR288suxKdU
    HhJVU1pZuKiSJ4p9Tj511N9J8IcbdyAHmWVdat9RaQc4
    UKwARCDJCXAXnEwMx+Afh9mB4EN5kFFLL1PLb06BF4Js
    QjVjsMqWUCzcXhdPP2bj9PRjvhH1Jh4cA== )

;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Sun Oct 29 20:55:07 CET 2017
;; MSG SIZE rcvd: 1477

root@athos:~#

```

Como vemos, obtenemos respuesta, la consulta se la hicimos al servidor secundario y de forma recursiva, lo que quiere decir que ambos funcionan como se esperaba.

## Parte 4: Apache directiva options:

Options controla las funcionalidades disponibles en un directorio en particular. Se puede establecer a “None” lo que hará que ninguna de las funcionalidades sean aplicadas.

La directiva options de apache tiene varias opciones que enumeraremos a continuación.

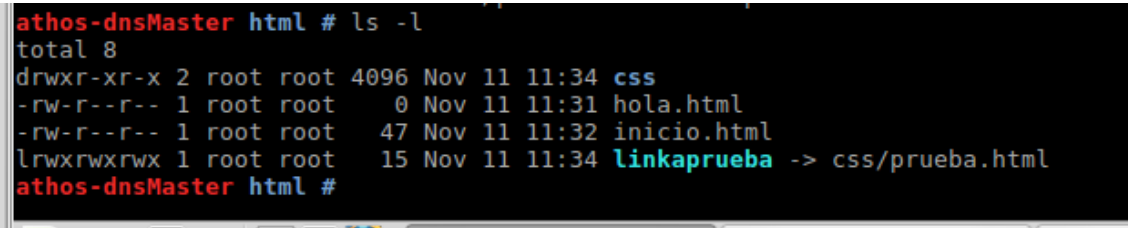
- All -> incluye todas las opciones menos Multiviews (all es la opción por defecto)
- ExecCGI -> Permite o no, la ejecución de scripts cgi
- FollowSymLinks -> Permite o no que se puedan seguir enlaces
- Includes -> Permite o no que se pueda utilizar mod\_include
- IncludesNOEXEC -> igual que la anterior, pero no permite la ejecución de comandos exec y exec cgi
- Indexes -> Permite o no que se muestren los archivos contenidos en un directorio cuando no se ha cargado ningún archivo específico, sino un directorio
- MultiViews -> permite o no, que cuando accedes a una url por ejemplo <http://ejemplo.com/prueba> en realidad cargue <http://ejemplo.com/prueba.html>
- SymLinksIfOwnerMatch El servidor solo permitirá seguir enlaces en los que el destino del enlace sea del mismo propietario que el propietario del enlace en si.

Estas opciones pueden ir o no precedidas del operador + o el operador -. Si no se pone el operador, y se especifican varias opciones, la opción más específica será usada mientras que el resto serán ignoradas. En cambio, si estas opciones son precedidas de un operador, todas las opciones serán “mezcladas”.

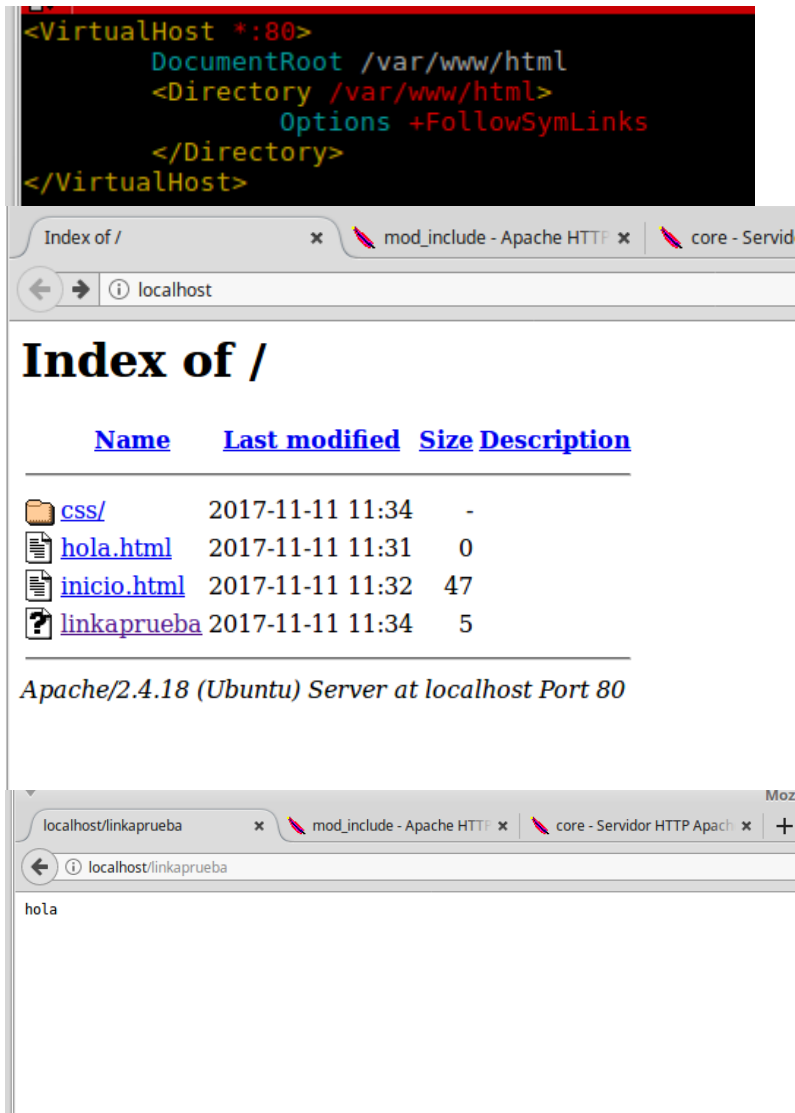
Ejemplos:

FollowSymLinks:

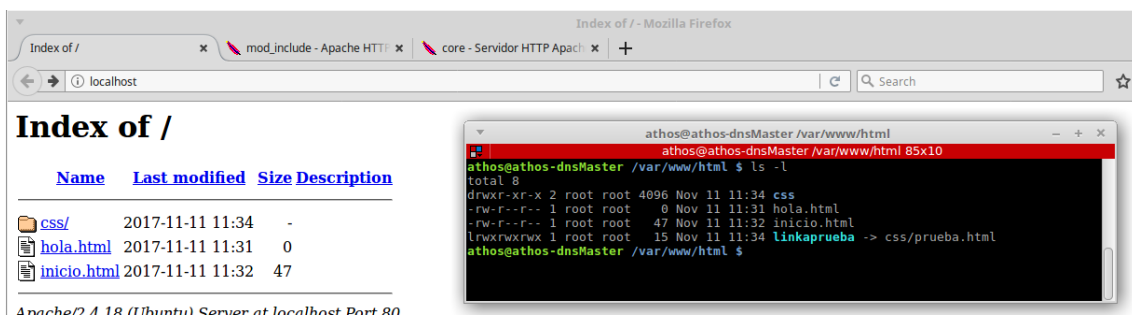
Con +FollowSymLinks vemos los enlaces, y podemos entrar en ellos



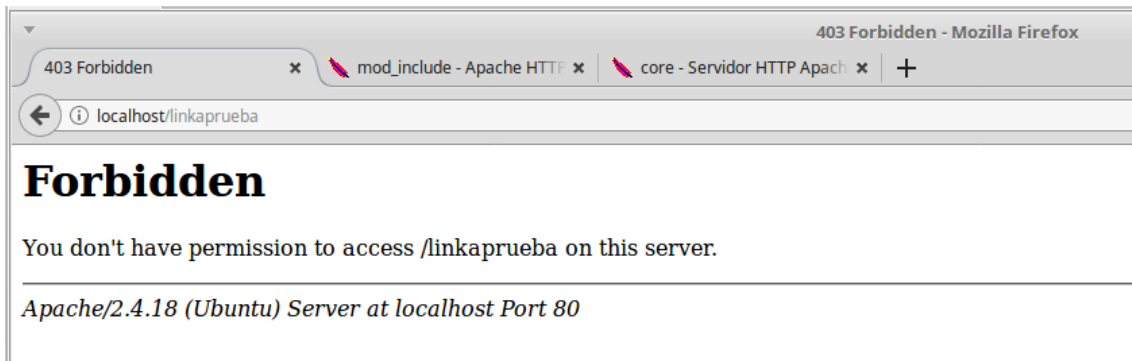
```
athos-dnsMaster html # ls -l
total 8
drwxr-xr-x 2 root root 4096 Nov 11 11:34 css
-rw-r--r-- 1 root root  0 Nov 11 11:31 hola.html
-rw-r--r-- 1 root root 47 Nov 11 11:32 inicio.html
lrwxrwxrwx 1 root root 15 Nov 11 11:34 linkaprueba -> css/prueba.html
athos-dnsMaster html #
```



En cambio si ponemos -FollowSymLinks ni siquiera los vemos

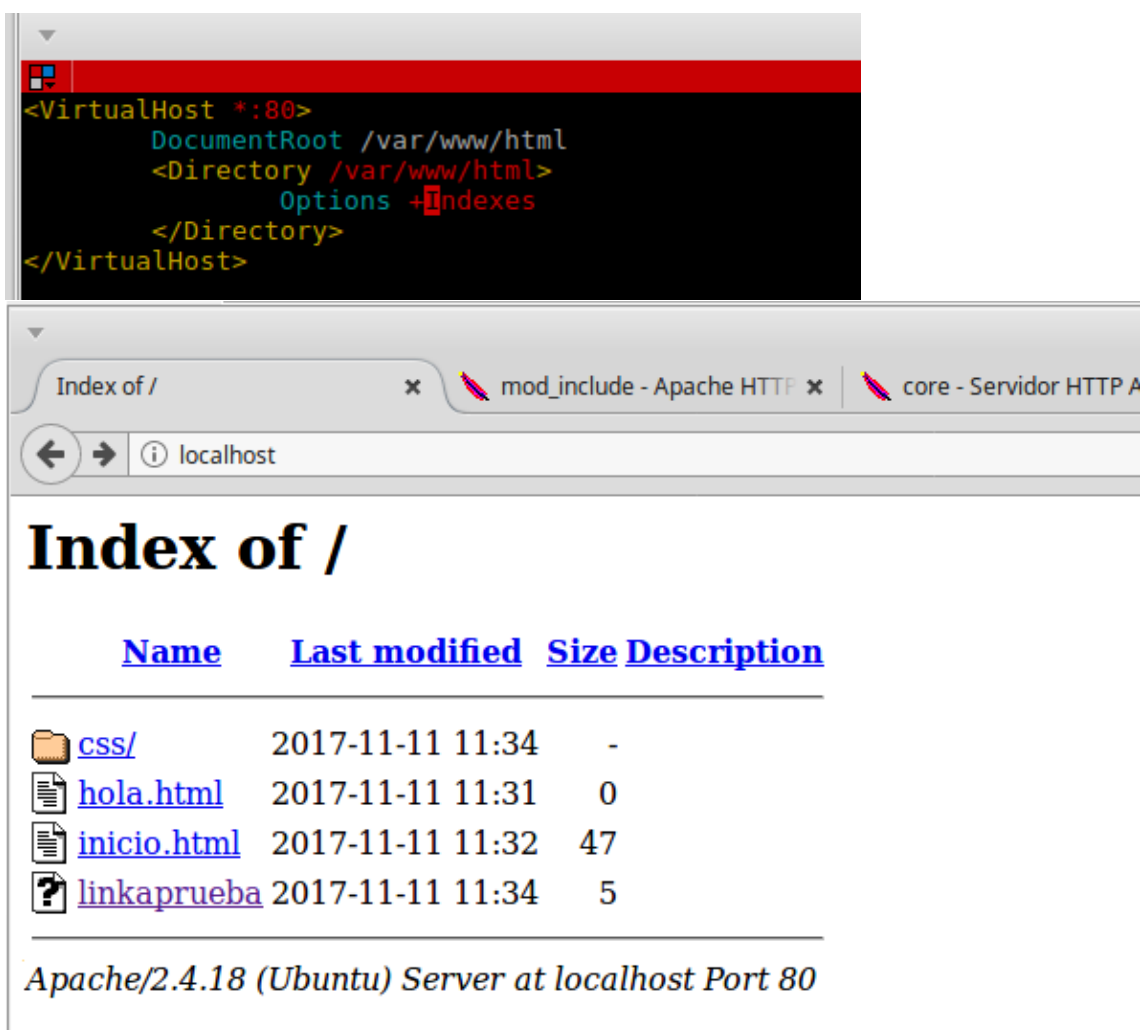


Y si intentamos entrar porque conocemos el nombre del enlace tampoco nos deja



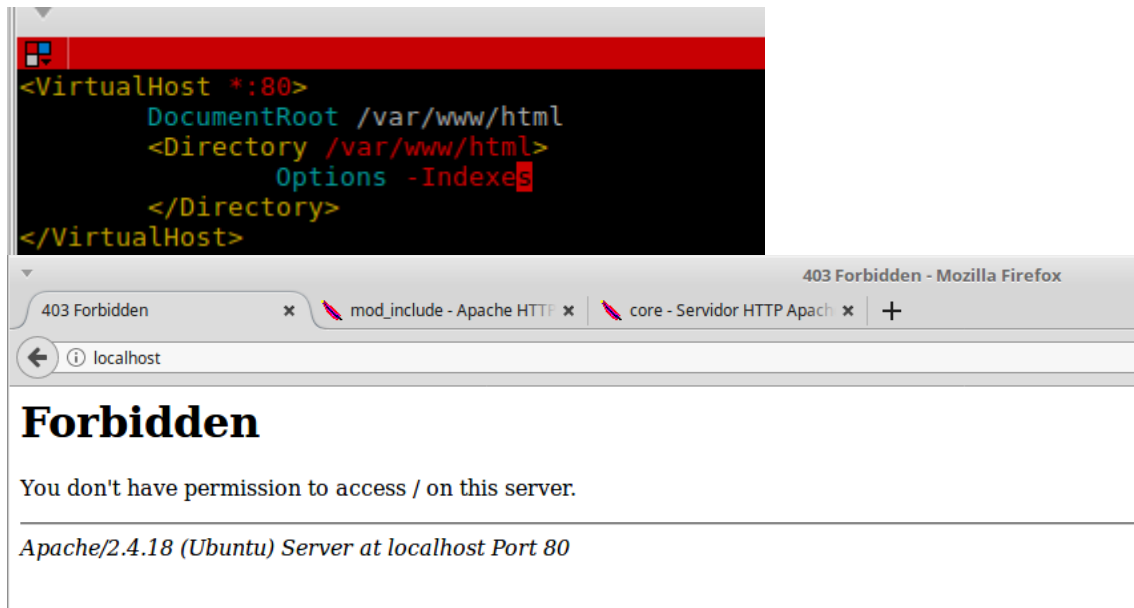
Indexes (por defecto activado)

Si no especificamos nada o lo activamos (+) podemos ver los archivos del directorio



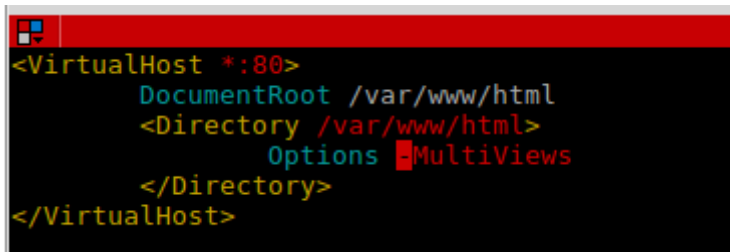


Si lo desactivamos, comprobaremos que ya no podemos ver el listado de archivos que hay en un directorio

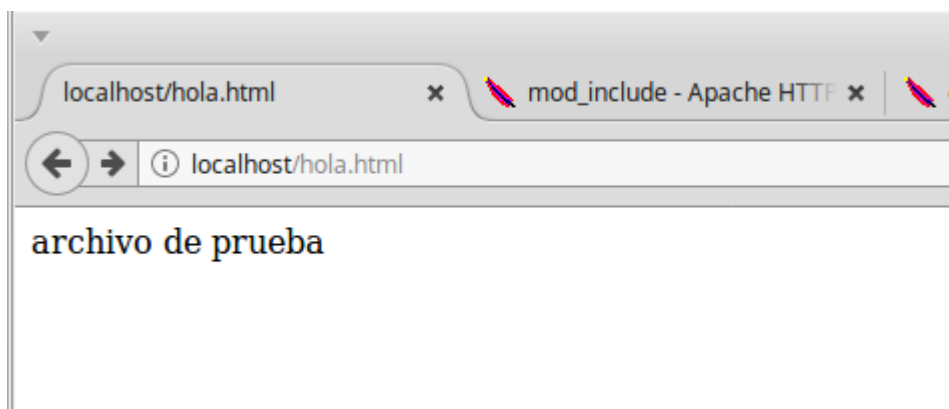


MultiViews: Por defecto desactivado

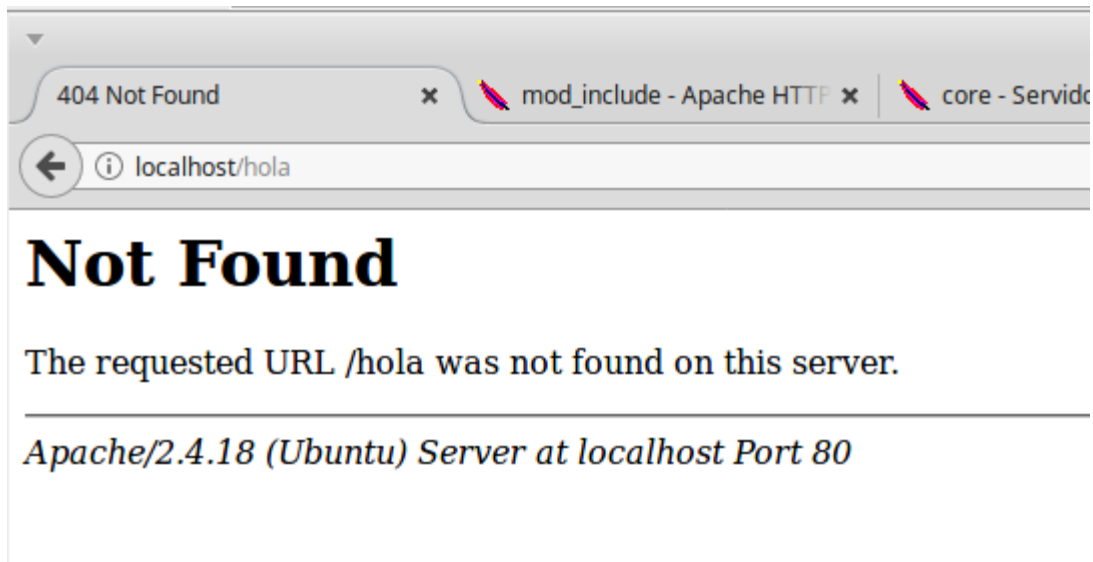
Si lo desactivamos o no ponemos nada



Podremos acceder a <http://localhost/hola.html>



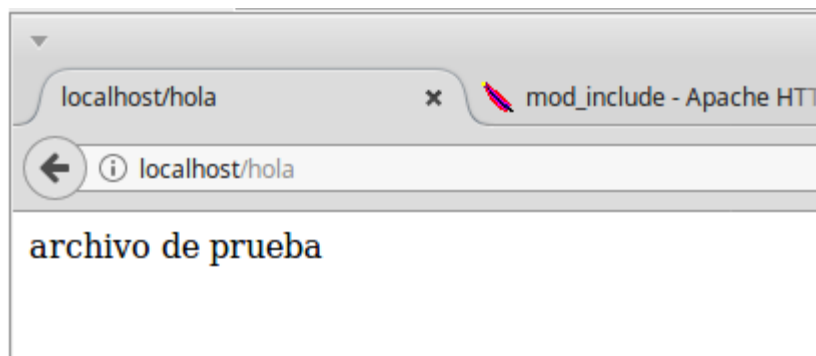
Pero no a <http://localhost/hola>



En cambio sí lo activamos:

```
<VirtualHost *:80>
    DocumentRoot /var/www/html
    <Directory /var/www/html>
        Options +MultiViews
    </Directory>
</VirtualHost>
```

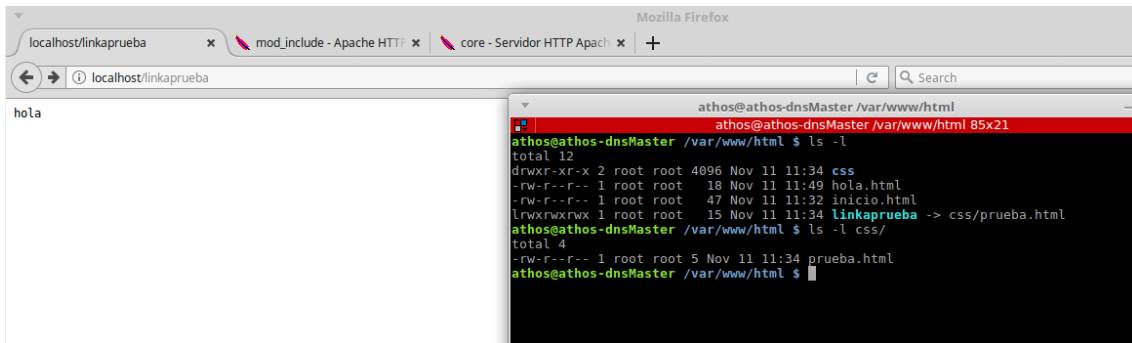
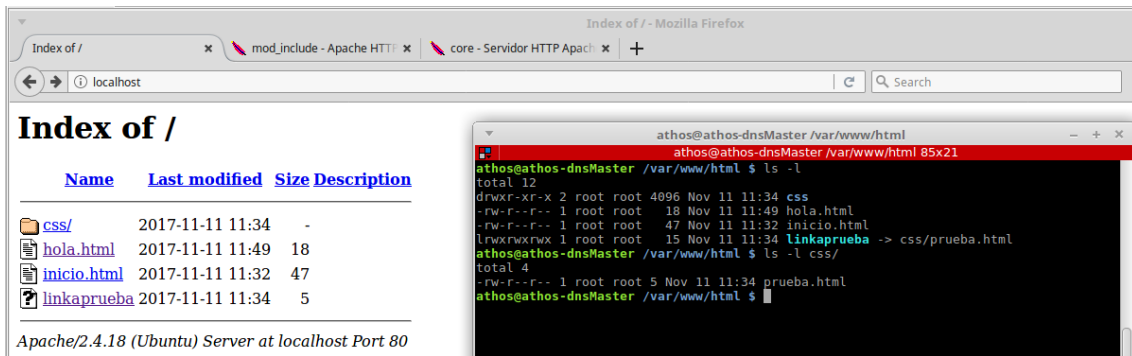
Si podremos acceder sin poner la extensión



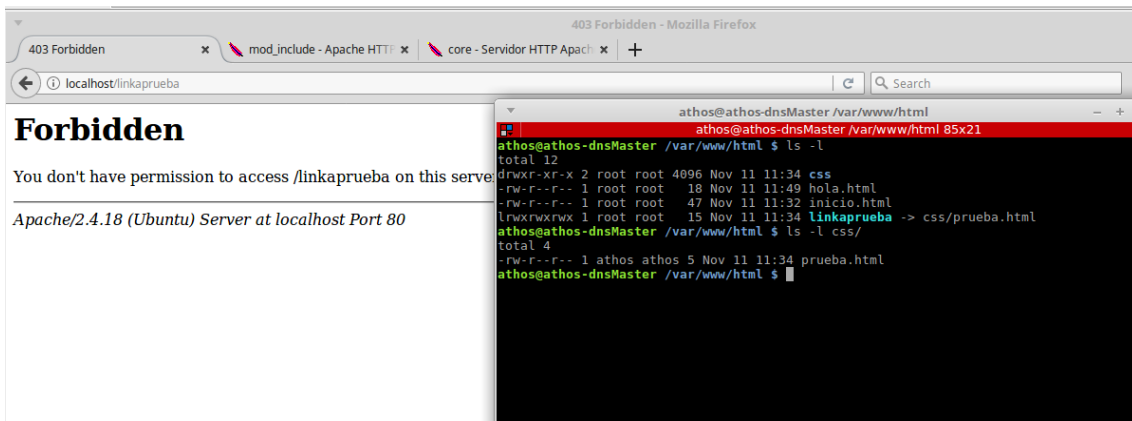
SymLinksIfOwnerMatch:

```
<VirtualHost *:80>
    DocumentRoot /var/www/html
    <Directory /var/www/html>
        Options +SymLinksIfOwnerMatch
    </Directory>
</VirtualHost>
```

Como el propietario de linkaprueba y de prueba.html son el mismo (root) si intentamos seguir el enlace podemos ver el contenido de prueba.html



En cambio si el propietario no coincide no nos deja ver el contenido



[http://www.microhowto.info/howto/configure\\_bind\\_as\\_a\\_slave\\_dns\\_server.html](http://www.microhowto.info/howto/configure_bind_as_a_slave_dns_server.html)

<https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2>