Seguridad en Redes
Practica 4.3

David Antuña Rodríguez
Javier Carrión García

1 Consultas recursivas DNSSEC

Salida:

```
www.example.com@8.8.8.8 (Google):
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.5 <<>> A +additional +multilin
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20509
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.example.com.        IN A

;; ANSWER SECTION:
www.example.com.         17527 IN A 93.184.216.34
www.example.com.         17527 IN RRSIG A 8 3 86400 20180528165149 (
   20180507220712 30381 example.com.
   EsLJLNCADwZG0G+75lsXGihaxoyBNv6VTt52xLsyTlrj
   kZ7hNowb9LSAeotStuqXSp2hA3KLJ5p0Tf+Lm6xFctfz
   /JTW3E89VXFKSYFhL5HCbERtvGOzyhUwY7p4ODpUmxed
   SDdi1JSaI2nlwGahWcZOXoGXs7crAiHnwWkgSG4= )

;; Query time: 1 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue May 22 12:21:53 2018
;; MSG SIZE  rcvd: 231
```

En RRSIG

- Tipo de registro: A
- Algoritmo de firma digital: RSA/SHA-256
- Componentes del dominio: 3
- TTL: 86400
- Fecha de expiracion: 28/05/2018
- Fecha de firma: 07/05/2018
- ID clave de firma: 30381
- Nombre del dominio: example.com.

- Firma digital en base 64:
  EsLJLNCADwZG0G+75lsXGihaxoyBNv6VTt52xLsyTlrj
  kZ7hNowb9LSAeotStuqXSp2hA3KLJ5p0Tf+Lm6xFctfz
  /JTW3E89VXFKSYFhL5HCbERtvGOzyhUwY7p4ODpUmxed
  SDdi1JSaI2nlwGahWcZOXoGXs7crAiHnwWkgSG4=

2 Consultas iterativas DNSSEC

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.5 <<>> A +additional +multilin
;; global options: +cmd
.                       28640 IN NS a.root-servers.net.
.                       28640 IN NS b.root-servers.net.
.                       28640 IN NS c.root-servers.net.
.                       28640 IN NS d.root-servers.net.
.                       28640 IN NS e.root-servers.net.
.                       28640 IN NS f.root-servers.net.
.                       28640 IN NS g.root-servers.net.
.                       28640 IN NS h.root-servers.net.
.                       28640 IN NS i.root-servers.net.
.                       28640 IN NS j.root-servers.net.
.                       28640 IN NS k.root-servers.net.
.                       28640 IN NS l.root-servers.net.
.                       28640 IN NS m.root-servers.net.
.                       28640 IN RRSIG NS 8 0 518400 20180601050000 (
        20180519040000 39570 .
        pY2wDGRT2c9FTU2ET0cHqIPJ048j/gzhTUImew3hsF92
        uiPVH4sDQjZUfkfNp7GOog4uLOQRj1AU3WC2H1GyCLx0
        0gxrcgUTgCJLxQjT5x33Ar6wF6OgTFjbnTnIa2388VCn
        KDYAL9qBaES50jwQEavqrHoZLlngrRNvxZ3QGQ+TfEIU
        z4vfKyxElx6wpbiOcUw4caerDxBVque9EkBtuXx8ixzZ
        PVs8bsNXkfkcgkKUViB5goBiMeRWZZNd+WRjyH3ZyjIJ
        h6kXmn70ncBiR6U0zqTfCq+pzx7y8YBpehXrL6qLHrHA
        wBCvUX2dvyGHQt3q6JNKhJDea9elqQnLHg== )
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 5 ms

com.                    172800 IN NS l.gtld-servers.net.
com.                    172800 IN NS d.gtld-servers.net.
com.                    172800 IN NS a.gtld-servers.net.
com.                    172800 IN NS j.gtld-servers.net.
com.                    172800 IN NS h.gtld-servers.net.
com.                    172800 IN NS b.gtld-servers.net.
com.                    172800 IN NS m.gtld-servers.net.
com.                    172800 IN NS g.gtld-servers.net.
com.                    172800 IN NS e.gtld-servers.net.
com.                    172800 IN NS c.gtld-servers.net.
com.                    172800 IN NS k.gtld-servers.net.
com.                    172800 IN NS f.gtld-servers.net.
com.                    172800 IN NS i.gtld-servers.net.
com.                    86400 IN DS 30909 8 2 (
        E2D3C916F6DEEAC73294E8268FB5885044A833FC5459
        588F4A9184CFC41A5766 )
com.                    86400 IN RRSIG DS 8 1 86400 20180604050000 (
        20180522040000 39570 .
        jXYmL0nVUHnwgGOdBUfx97tmMHKNSAyxHgPqx9Fb2kJU
        /Uv4aGZDjD3WDdYs0pD9Nnd29BjbT1gZyKC6gFRdtCjy
        uhH2aHfCKD8c/pTfLEDCGeYkkArKwiUL84X28zzcLtkH
        27sBcZPuH2i09CfghmT3BaycuP6P/WulY36yFv4nfuNB
        RatYGRw8qnKaPkPlMdmW6UQEPwIuXtCXO4l3Duy1961a
        XA2+hctjI/b9vpjl3gJC0pDzPdqiHhIe9MVmNrwsjEoC
        RbYrSWim+gSvoXROLRDL8i1VZDbh3t+4HQO0L4pq3yzw
        PWq4ccIC7az0VDrMMg/IorzkdTNacN/HUA== )
;; Received 1175 bytes from 192.112.36.4#53(192.112.36.4) in 26 ms

example.com.            172800 IN NS a.iana-servers.net.
example.com.            172800 IN NS b.iana-servers.net.
example.com.            86400 IN DS 31589 8 1 (
        3490A6806D47F17A34C29E2CE80E8A999FFBE4BE )
example.com.            86400 IN DS 31589 8 2 (
        CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA
        59875A990C03E576343C )
example.com.            86400 IN DS 43547 8 1 (
        B6225AB2CC613E0DCA7962BDC2342EA4F1B56083 )
example.com.            86400 IN DS 43547 8 2 (
        615A64233543F66F44D68933625B17497C89A70E858E
        D76A2145997EDF96A918 )
example.com.            86400 IN DS 31406 8 1 (
        189968811E6EBA862DD6C209F75623D8D9ED9142 )
example.com.            86400 IN DS 31406 8 2 (
        F78CF3344F72137235098ECBBD08947C2C9001C7F6A0
        85A17F518B5D8F6B916D )
example.com.            86400 IN RRSIG DS 8 2 86400 20180527042417 (
        20180520031417 36707 com.
        RBarp4dfMz8caraD+4L/vpTltysxnrLyVC6eDXDfq+vY
        6D6QDNE6TdG16OyiTQcPjvIfRkqu3mjGRIDK3NUNs5Y7
        Ifk+XqJgy9rdy3WrUdt353l/lifPo7i0mRVwJAgjkeeA
        g3Evz4mEEfqu0m4lJFtY3MjGK7wcVESUSTzHtoc= )
```

```
;; Received 595 bytes from 192.52.178.30#53(192.52.178.30) in 21 ms

www.example.com.            86400 IN A 93.184.216.34
www.example.com.            86400 IN RRSIG A 8 3 86400 20180612053429 (
            20180522075626 4354 example.com.
            AkEbv0lUfyjLr8puN8f+qDgGhJU4gQHvYtcNet7iqdkZ
            wQcQDhlFxCsdr140TzItKWHUWyv+z1A+3jWrpoIWYOz/
            o8ekEgefFhAmk9GpiDfeE7nMuDqDupe3JEqZYu+nxrKw
            M8JQkZ7+ijw/BSokvbKvS+nMmPzw2/wVk4iDs60= )
example.com.                86400 IN NS b.iana-servers.net.
example.com.                86400 IN NS a.iana-servers.net.
example.com.                86400 IN RRSIG NS 8 2 86400 20180612105904 (
            20180522075626 4354 example.com.
            R72G9nNtxkqS/bJEZPSsMzeAdnYeU4aRykn5ZbZxZwT9
            hVBeZMY+1SvSbaT8KeMk1tbHQRZIhkdpuDUNwSlBJmPk
            kpCbnL/XCsJfeuTGaNwzXugztysW3f6K6e1mwqxhPXwu
            +qKuA1kNJJFE2hGKwi/Go/U6Y1j44Ln4A8W/sJM= )
;; Received 538 bytes from 199.43.133.53#53(199.43.133.53) in 51 ms
```

Registro DS de la zona **com.**

- Id clave: 30909
- Algoritmo de firma digital: RSA/SHA-256
- Algorimo de resumen: SHA-256
- Resumen en base64:
  E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

Registro DS de la zona **example.com.**

- Id clave: 31589
- Algoritmo de firma digital: RSA/SHA-256
- Algorimo de resumen: SHA-1
- Resumen en base64:
  3490A6806D47F17A34C29E2CE80E8A999FFBE4BE

Registro DS de la zona **example.com.**

- Id clave: 31589
- Algoritmo de firma digital: RSA/SHA-256

- Algorimo de resumen: SHA-256
- Resumen en base64:
  CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03E576343C

Registro DS de la zona **example.com.**

- Id clave: 43547
- Algoritmo de firma digital: RSA/SHA-256
- Algorimo de resumen: SHA-1
- Resumen en base64:
  B6225AB2CC613E0DCA7962BDC2342EA4F1B56083

Registro DS de la zona **example.com.**

- Id clave: 43547
- Algoritmo de firma digital: RSA/SHA-256
- Algorimo de resumen: SHA-256
- Resumen en base64:
  615A64233543F66F44D68933625B17497C89A70E858ED76A2145997EDF96A918

Registro DS de la zona **example.com.**

- Id clave: 31406
- Algoritmo de firma digital: RSA/SHA-256
- Algorimo de resumen: SHA-256
- Resumen en base64:
  F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D8F6B916D

3 Claves DNSSEC

Zona **.**

- ID clave KSK: 19036 y 20326
- ID clave ZSK: 39570

Zona **com.**

- ID clave KSK: 30909
- ID clave ZSK: 36707

Zona **example.com.**

- ID clave KSK: 45620 y 31406
- ID clave ZSK: 30381 y 4354

Los registros DS validos de cada zona son los que emplean las siguientes firmas:

- *com.* emplea la firma KSK con id 30909
- *example.com.* utililza la firma KSK con id 31406.

En el registro RRSIG de:

- . utiliza su propia ZSK con id 39570.
- *com.* utiliza la ZSK de . con id 39570.
- *example.com.* se emplea la ZSK de *com.* 36707.
- *www.example.com* la ZSK pertenece a *example.com.* con id 4354.

4 Validación de firmas DNSSEC

1. Verifica .

```
;; Ok, find a Trusted Key in the DNSKEY RRset: 19036
;; VERIFYING DNSKEY RRset for . with DNSKEY:19036: success

;; We are in a Grand Father Problem: See 2.2.1 in RFC 3568
;; and we try to continue chain of trust validation of the zone: com.
```

2. Verifica com.

```
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for com. with DNSKEY:30909: success

;; We are in a Grand Father Problem: See 2.2.1 in RFC 3568
;; and we try to continue chain of trust validation of the zone: example.com.
```

3. Verifica example.com.

```
;; VERIFYING DS RRset for example.com. with DNSKEY:36707: success
```

4. Respuesta

```
www.example.com.          17831   IN      A       93.184.216.34


;; FINISH : we have validate the DNSSEC chain of trust: SUCCESS
```

5 Negación de existencia autenticada DNSSEC

Respuesta:

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> fake.verisign.com A +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59493
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;fake.verisign.com.             IN      A

;; AUTHORITY SECTION:
verisign.com.             1799    IN      SOA     av1.nstld.com. mdnshelp.verisi
verisign.com.             1799    IN      RRSIG   SOA 8 2 86400 20180531204359 2
LVNT2DK6E38UB5HG27E7MCINT8M21C9P.verisign.com. 21599 IN NSEC3 1 0 8 4C44934802
LVNT2DK6E38UB5HG27E7MCINT8M21C9P.verisign.com. 21599 IN RRSIG NSEC3 8 3 86400
ip7epa1q9p34q9bm9vs1b6ka333kbv1b.verisign.com. 21599 IN NSEC3 1 0 8 4C44934802
ip7epa1q9p34q9bm9vs1b6ka333kbv1b.verisign.com. 21599 IN RRSIG NSEC3 8 3 86400
2p7gpdk6gmc6l7vnmq3tbj1pnnpfrlvn.verisign.com. 21599 IN NSEC3 1 0 8 4C44934802
2p7gpdk6gmc6l7vnmq3tbj1pnnpfrlvn.verisign.com. 21599 IN RRSIG NSEC3 8 3 86400

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue May 22 13:18:12 2018
;; MSG SIZE  rcvd: 1045
```

Aparecen 3 registros NSEC3, la diferencia entre el campo de nombres de propietario resumido es que ne NSEC ves los nombres de las zonas y en NSEC3 no.

6 Transferencia de zonas DNS

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.5 <<>> AXFR +additional +mult
;; global options: +cmd
zonetransfer.me.        7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. (
        2017103001 ; serial
        172800     ; refresh (2 days)
        900        ; retry (15 minutes)
        1209600    ; expire (2 weeks)
        3600       ; minimum (1 hour)
        )
zonetransfer.me.        300 IN HINFO "Casio fx-700G" "Windows XP"
zonetransfer.me.        301 IN TXT "google-site-verification=tyP28J7JAUHA9fw2s
zonetransfer.me.        7200 IN MX 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200 IN MX 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200 IN MX 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200 IN MX 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200 IN MX 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200 IN MX 20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200 IN A 217.147.177.157
zonetransfer.me.        7200 IN NS nsztm1.digi.ninja.
zonetransfer.me.        7200 IN NS nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN SRV 0 0 5060 www.zonetransfer.me.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me
asfdbauthdns.zonetransfer.me. 7900 IN AFSDB 1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200 IN A 127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN AFSDB 1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A 202.14.81.230
cmdexec.zonetransfer.me. 300 IN TXT "\; ls"
contact.zonetransfer.me. 2592000 IN TXT "Remember to call or email Pippa on +
dc-office.zonetransfer.me. 7200 IN A 143.228.181.132
deadbeef.zonetransfer.me. 7201 IN AAAA dead:beaf::
dr.zonetransfer.me.     300 IN LOC 53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000
DZC.zonetransfer.me.    7200 IN TXT "AbCdEfG"
email.zonetransfer.me.  2222 IN NAPTR 1 1 "P" "E2U+email" "" email.zonetransf
email.zonetransfer.me.  7200 IN A 74.125.206.26
home.zonetransfer.me.   7200 IN A 127.0.0.1
Info.zonetransfer.me.   7200 IN TXT "ZoneTransfer.me service provided by Robin
internal.zonetransfer.me. 300 IN NS intns1.zonetransfer.me.
internal.zonetransfer.me. 300 IN NS intns2.zonetransfer.me.
intns1.zonetransfer.me. 300 IN A 81.4.108.41
intns2.zonetransfer.me. 300 IN A 52.91.28.78
office.zonetransfer.me. 7200 IN A 4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA 2001:67c:2e8:11::c100:1332
```

```
owa.zonetransfer.me.      7200 IN A 207.46.197.32
robinwood.zonetransfer.me. 302 IN TXT "Robin Wood"
rp.zonetransfer.me.       321 IN RP robin.zonetransfer.me. robinwood.zonetransf
sip.zonetransfer.me.      3333 IN NAPTR 2 3 "P" "E2U+sip" "!^.*$!sip:customer-s
sqli.zonetransfer.me.     300 IN TXT "' or 1=1 --"
sshock.zonetransfer.me. 7200 IN TXT "() { :]}\; echo ShellShocked"
staging.zonetransfer.me. 7200 IN CNAME www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.
vpn.zonetransfer.me.      4000 IN A 174.36.59.154
www.zonetransfer.me.      7200 IN A 217.147.177.157
xss.zonetransfer.me.      300 IN TXT "'><script>alert('Boo')</script>"
zonetransfer.me.          7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. (
       2017103001 ; serial
       172800     ; refresh (2 days)
       900        ; retry (15 minutes)
       1209600    ; expire (2 weeks)
       3600       ; minimum (1 hour)
       )
;; Query time: 21 msec
;; SERVER: 52.91.28.78#53(52.91.28.78)
;; WHEN: Tue May 22 13:27:52 2018
;; XFR size: 48 records (messages 1, bytes 1878)
```