Aleksandr Kurganov, 123RF

The sys admin's daily grind: dig

Dig It

Many administrators rely on Linux tools whose fate is already sealed, but external forces can help people let go of old habits. *By Charly Kühnast*

Most administrators will be aware that `ifconfig`'s days are numbered; after all, the `ip` command is far more powerful – and saves typing into the bargain! I'm aware of this, too, but I still find myself using the legacy tool. The same thing happens to me with the good old `nslookup`. The heir to its throne, `dig`, is a diagnostic tool for nameserver issues. Despite this, the `dig` utility [1] still struggles to compete with its ancestor.

Because of the normative force of fact, however, things are starting to change: The most comprehensive protocol extension in the history of the Domain Name System (DNS) is currently in full swing. I'm talking about DNSSEC.

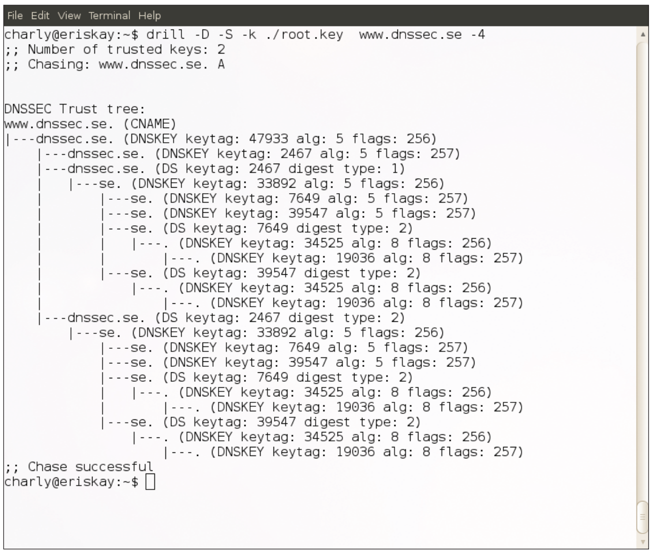
These security extensions support the signing of zone information and could help put an end to DNS spoofing. DNSSEC [2] creates a chain of trust that starts in the root zone and extends through the generic (`.com`, `.net`, etc.) and country domains (`.fr`, `.de`, etc.) and continues down through the hierarchical structure of DNS.

The root zone, which is represented by a dot (`.`) in the DNS nomenclature, added the required signatures midyear in 2010. By the time this magazine reaches newsstands, the `.de` zone should have joined suit – the test period was due to end May 31.

Digging Dig

So, if I want to find out whether a specific domain is signed, `nslookup` will not help me, because it doesn't support DNSSEC. But `dig` does, so I can enter:

```
dig NS ns1.nic.fr +dnssec
```


File Edit View Terminal Help

```
charly@eriskay:~$ drill -D -S -k ./root.key  www.dnssec.se -4
;; Number of trusted keys: 2
;; Chasing: www.dnssec.se. A


DNSSEC Trust tree:
www.dnssec.se. (CNAME)
|---dnssec.se. (DNSKEY keytag: 47933 alg: 5 flags: 256)
    |---dnssec.se. (DNSKEY keytag: 2467 alg: 5 flags: 257)
    |---dnssec.se. (DS keytag: 2467 digest type: 1)
    |   |---se. (DNSKEY keytag: 33892 alg: 5 flags: 256)
    |       |---se. (DNSKEY keytag: 7649 alg: 5 flags: 257)
    |       |---se. (DNSKEY keytag: 39547 alg: 5 flags: 257)
    |       |---se. (DS keytag: 7649 digest type: 2)
    |       |   |---. (DNSKEY keytag: 34525 alg: 8 flags: 256)
    |       |       |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
    |       |---se. (DS keytag: 39547 digest type: 2)
    |           |---. (DNSKEY keytag: 34525 alg: 8 flags: 256)
    |               |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
    |---dnssec.se. (DS keytag: 2467 digest type: 2)
        |---se. (DNSKEY keytag: 33892 alg: 5 flags: 256)
            |---se. (DNSKEY keytag: 7649 alg: 5 flags: 257)
            |---se. (DNSKEY keytag: 39547 alg: 5 flags: 257)
            |---se. (DS keytag: 7649 digest type: 2)
            |   |---. (DNSKEY keytag: 34525 alg: 8 flags: 256)
            |       |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
            |---se. (DS keytag: 39547 digest type: 2)
                |---. (DNSKEY keytag: 34525 alg: 8 flags: 256)
                    |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
;; Chase successful
charly@eriskay:~$ □
```

Figure 1: Charly uses drill to see whether the chain of trust in Sweden's DNS has a missing link.

The output doesn't just return the corresponding IP address, it also gives me the new `RRSIG` records, which contain the signature data, thanks to `+dnssec`. The public keys required for validation are now stored directly in the zone. To allow this to happen, a `DNSKEY` record is needed. If I want to retrieve the public key for the root zone and write it to my `root.key` file, I need to enter the following line:

```
dig DNSKEY . +dnssec > ./root.key
```

Armed with this information, I can trace the complete chain of trust into the root zone using another useful tool, `drill`, from the ldns-utils package [3]. In the following example, I do this for the Swedish website:

```
drill -D -S -k ./root.key www.dnssec.se
```

Figure 1 shows the chain of trust in an easily understandable ASCII graphic. My conclusion is that you sometimes need external pressure to be able to let go of old habits. Rest in peace, `nslookup`. ■■■

INFO

[1] dig man page: *http://linux.die.net/man/1/dig*

[2] DNSSEC: *http://www.dnssec.net/*

[3] ldns: *http://www.nlnetlabs.nl/projects/ldns/*

AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.