

DNS

Andrea Leofreddi

July 16, 2003

Contents

1	Example zone configuration for mydomain.com	2
2	BIND version query	2
3	Secure BIND configuration	3

1 Example zone configuration for mydomain.com

```
$TTL      172800
@         IN      SOA      mydomain.com. admin.mydomain.com. (
                        200306210      ; Serial
                        604800         ; Refresh
                        86400          ; Retry
                        604800         ; Expire
                        21600 )         ; TTL

; zone NS/MX
@         IN      NS       ns1
@         IN      NS       ns2

@         IN      MX       10    mail1
@         IN      MX       20    mail2

; nameservers
ns1       IN      A        128.1.1.1
ns2       IN      A        128.1.1.2

; mailservers
mail1     IN      A        128.1.1.3
mail2     IN      A        128.1.1.4

; webservers
www       IN      A        128.1.2.40
www       IN      A        128.1.2.41
www       IN      A        128.1.2.42
www       IN      A        128.1.2.43

; experimental ipv6 server
www       IN      AAAA     3ffe:ffff:54de:4d3d::4

; subdomains
sub       IN      NS       ns1.sub
sub       IN      NS       ns2.sub
ns1.sub   IN      A        128.1.1.5
ns2.sub   IN      A        128.1.1.6
```

2 BIND version query

Using *nslookup*, you can easily get server BIND version:

```
nslookup -q=txt -class=CHAOS version.bind. [dns server]
```

3 Secure BIND configuration

With a little effort, you can enhance BIND security. In *named.conf*, under *options* section, you can add:

1. `version "this should not interest you";`
to make BIND fake its version since there's not a good reason to let users know which dns software/version you are running.
2. `recursion no;`
to disallow recursion on this server, since recursive queries can hide a security hole.
3. `allow-transfer { none; };`
Transfer zone can lead high bandwidth usage and can help malicious users to find more information about our network.

Other things you can do are:

1. run BIND in a *chroot()* environment using *-t* flag
2. make BIND drop root privileges using *-u* flag