Table of Contents

Membuat Database Spammer dengan RBLDNS

Kali ini kami membuat database spammer dengan rbldns yang kami jalankan pada sistem operasi Almalinux

```
yum install epel-release -y
yum install rbldnsd -y
```

Setelah dua paket tersebut terinstall selanjutnya membuat konfigurasi

```
mkdir /etc/rbldnsd -p
nano /etc/sysconfig/rbldnsd
```

isi dengan

```
OPTIONS="-u rbldns -p /var/run/rbldnsd.pid -f -r /etc/rbldnsd \
        -b ip_address_server \
        rbl.serveranda.net:ip4set:default,blacklist,whitelist \
        rbl.serveranda.net:dnset:domain_blacklist \
        "
```

kemudian pada default isi dengan

```
nano /etc/rbldnsd/default
```

isi dengan

```
#------------------------------
:127.0.0.2:Open relay, see http://relays.example.com/lookup?$
# The above is a default or implicit value which is used when no value given
# for an entry.  The `$' characters will be replaced by an IP address in
# question.
127.0.0.2
# A simplest case: single IP address, with default value.
10.8.60.0/24 :127.0.0.3:Address $ is from a private IP range

# Netblock - 256 IP addresses with their own A and TXT records
224/4        Reserved multicast address
# Another netblock, with default A and explicit TXT values.
192.168  Dialup pool, see http://dialups.example.com/lookup?$ for
explanations
# IP numbers may be abbreviated, the above is the same as 192.168.0.0/16
10.10    :5:This network blocked due to massive spam issues
# A value may be abbreviated as well - :5: is the same as :127.0.0.5:.
10.10.5-129     :5:Those hosts are nasty
# repeat last octet: 10.10.5.0..10.10.129.255 inclusive
```

```
!10.10.1.2
# exclusion entry
# exclusion entry
#
# The following examples are for name-based zones.
#yahoo.com   :2:This domain has no working postmaster@ address
#*.yahoo.com :2:All subdomains of example.com lacks working abuse@ address
# Simple and wildcarded entry, both will return 127.0.0.2 A record
#
# some specials
$SOA 3000 ns1.serveranda.net admin.serveranda.net 0 600 300 86400 300
# Start of authority record (TTL 3000), with serial (0) computed as
# a timestamp of data file
$NS 3000 ns1rbl.serveranda.net ns2rbl.serveranda.net
# two nameservers
```

Kemudian anda bisa membuat record dns pada domain ns1rbl dan ns2rbl.serveranda.net dalam hal ini jika hanya memiliki 1 server saja, maka ip_address_server isinya sama

```
ns1rbl.serveranda.net. A ip_address_server
ns2rbl.serveranda.net. A ip_address_server
```

Kemudian buat NS pada rbl.serveranda.net

```
rbl.serveranda.net. NS ns1rbl.serveranda.net
rbl.serveranda.net. NS ns2rbl.serveranda.net
```

Demikian dan semoga bermanfaat

Referensi

1. https://linux.die.net/man/8/rbldnsd
2. https://www.surbl.org/rbldnsd-bind-freebsd
3. https://docs.farsightsecurity.com/nod-noh/nod-dnsbl-rsync-rbldnsd-howto/