Documentation and Manual for DNS configuration and implementation strategy.

# HOW NOT TO MESS UP

To implement this yourself its required the following:

#1 - Kali Linux OS VERSION=”2020.2” ID_LIKE=debian x64arch

#2 - Active Internet connection.

#3 - bind9 software installed. Check bind9 documentation.

#4 - IPV4 as standard protocol. Check ISP configuration.

#5 - Port53 open. Check the firewall or ISP configuration.

I highly suggest that you read this manual thoroughly before attempting any action. If you start modifying these files and then give up in the middle of these configurations you might lose internet access altogether.

**! Noobs Beware !**

!Warning: If it’s used wrong it can be dangerous.
If a wrong remote IP is in your configuration files, the attackers not only own all internet traffic but can also use it to steal your credentials. Check for “man in the middle attacks” for more information.

As such you must follow these rules:

#1) Respect the privacy of others.

#2) Think before you type.

#3) With great power comes great responsibility.

If bind9 is not installed then in the terminal type:
`sudo apt-get install bind9`

Then find out what your internal IP address is. In the terminal type:
`ifconfig`

The following was the data used at the time of configuration. This is probably vastly different from yours.

My IP address at that time was 192.168.0.104.
The domain I wanted to use was *ns.dudechill.net*

This project will be using the network interface as the DNS server address.
The bind9 package on Debian-related distros don't ship with a *db.root* file. Now it uses the *root.hints* file. This file is used by DNS resolvers to query *root-servers.net*

The bind9 package provides with recursive service for local host and local network clients only. Outside queries are denied unless told the contrary.

The main BIND configuration file is */etc/bind/named.conf*
This files sources all its data from other three files in the same folder:

A) etc/bind/named.conf.options

B) etc/bind/named.conf.local

C) etc/bind/named/conf.default-zones

Go to the main configuration folder for bind. In the current version is in *etc/bind/*
Open the *named.conf.local* file and add the following:

```
zone    “dudechill.net” {
        type master;
        file “/etc/bind/db.forward.net”
};

zone    “0.168.192.in-addr.arpa” {
        type master;
        file “/etc/bind/db.reverse.net”;
};
```

This enables two different zones. One as forward and the other one as a reverse.
Now we must create these zones. For the forward zone I strongly suggest that you copy the *db.local* file to the same folder and rename it as “*db.forward.net*”.
Edit this file and try to have the same as the following:

```
;
; BIND data file for local loopback interface
;
$TTL604800
@   IN  SOA ns.dudechill.net. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@       IN  NS  ns.dudechill.net.
ns      IN  A   192.168.0.104
server  IN  A   192.168.0.104

###end of file
```

For the reverse zone I strongly suggest that you copy the *db.127* file to the same folder and rename it as "*db.reverse.net*"
Edit this file and try to have the same as the following:

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@   IN  SOA ns.dudechill.net. root.localhost. (
                    1      ; Serial
               604800      ; Refresh
                86400      ; Retry
              2419200      ; Expire
               604800 )    ; Negative Cache TTL
;
@   IN  NS  ns.
104 IN  PTR ns.dudechill.net.
104 IN  PTR server.dudechill.net.

###end of file
```

These two zones are now completely configured.

Warning: the number 104 used at the end of the file was my IP's last number, change accordingly. Check *ifconfig* if in doubt.

In reality it wasn't required to create the forward and reverse zone files, but as a safety measure its a highly recommended action.

Now outside the */bind* folder but still in */etc*, edit the *resolv.conf* file.

Here comment all nameservers you had previously and add:

```
nameserver 192.168.0.104
search dudechill.net
domain dudechill.net
###end of file
```

Now to run the bind process in the terminal type:
*etc/init.d/bind9 start*
it should display the following:
*[ok] Starting bind9 (via systemctl): bind9.service*

Now to check if the DNS name server is running flawlessly type:
*nslookup ns.dudechill.net*
it should display the following:

```
Server:         192.168.0.104
Address:        192.168.0.104#53

Name:           ns.dudechill.net
Address:        192.168.0.104
```

WARNING: A single typo in any configuration file is enough to lose all internet access. If in an emergency restore the */etc/resolv.conf* file to its default. This is related to the rule #2) above.