Configuration of DNS Server

(catching Recursion and forwarders)

Snapshot1 :
Change password for both root and shuhari user.
# nano /etc/apt/sources.list

```
deb [trusted=1] http://192.168.1.251/sw/repo/deb10/ buster main
deb http://deb.debian.org/debian buster main
```

#apt-get update
#apt-get install apache2 -y && apt-get install openssh-server -y && apt-get install sudo -y
#visudo

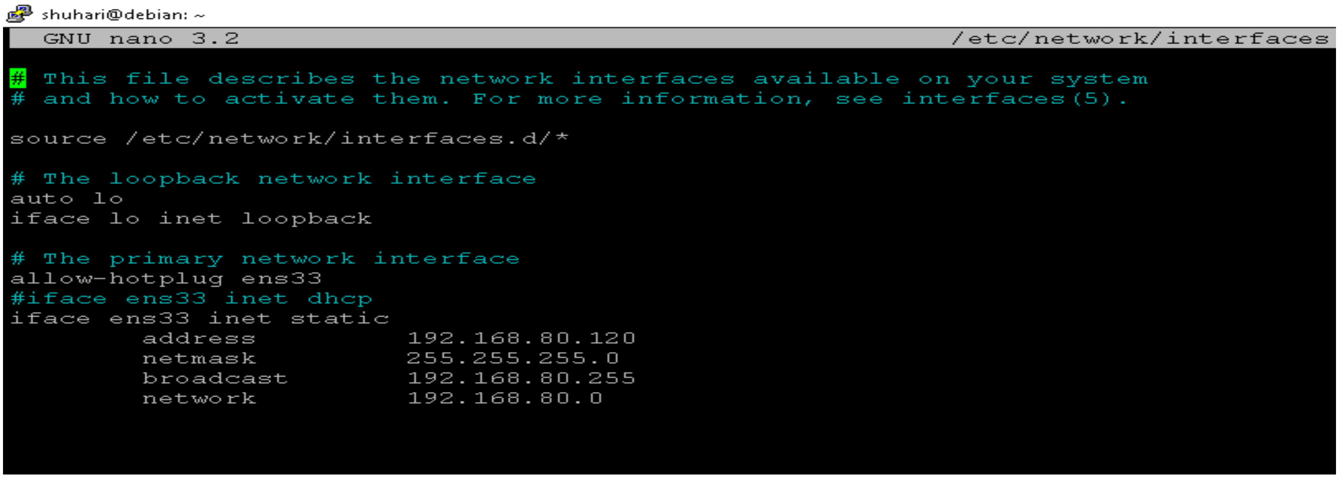
```
shuhari ALL(ALL:ALL)
```

Logout and login as shuhari and run any sudo command .

DNS : Domain name system port 53
1)
$ sudo apt-get install bind9 -y && sudo apt-get install bind9utils && sudo apt-get install dnsutils -y
(install necessary packages)*dynamic ip is required for this .
2) Configure static IP .(range 3-127)

a) Edit->network editor->change setting -> vmnet 8 or any adapter -> untick local dhcp server
(this we have done to turn off dhcp server or don't allow server to allocate dynamic ip)

b) Edit configuration file .
$ sudo nano /etc/network/interfaces. (ctrl+o -> enter -> ctrlX)



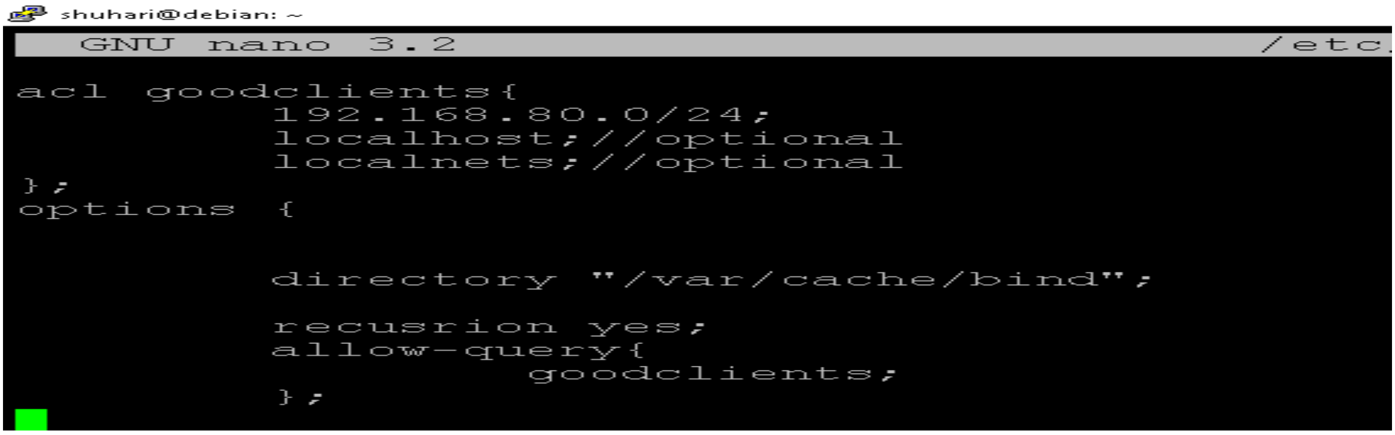
```
  GNU nano 3.2                                              /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
#iface ens33 inet dhcp
iface ens33 inet static
        address         192.168.80.120
        netmask         255.255.255.0
        broadcast       192.168.80.255
        network         192.168.80.0
```

$sudo reboot

C) Edit configuration files: (before editing ensure backup)
$ sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
$sudo nano /etc/bind/named.conf.options.

```
        acl goodclients {
        192.168.80.0/24;
        localhost;
        localnets;
};
```

Options-> directory->
Recursion yes; (A recursive DNS lookup is where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client.)



```
shuhari@debian: ~
  GNU nano 3.2                                         /etc

acl goodclients{
          192.168.80.0/24;
          localhost;//optional
          localnets;//optional
};
options {

          directory "/var/cache/bind";

          recusrion yes;
          allow-query{
                    goodclients;
          };
```

$sudo named-checkconf (to check error in configuratuion files)
$sudo systemctl restart bind9
$sudo systemctl status bind9 (active:running)
Checking:
D) VM Windows -> win+r->ncpa.cpl->ethernet properties ->ipv4->preferred dns server 8.8.8.8
E) VM windows -> cmd -> nslookup -> www.shuharilabs.com

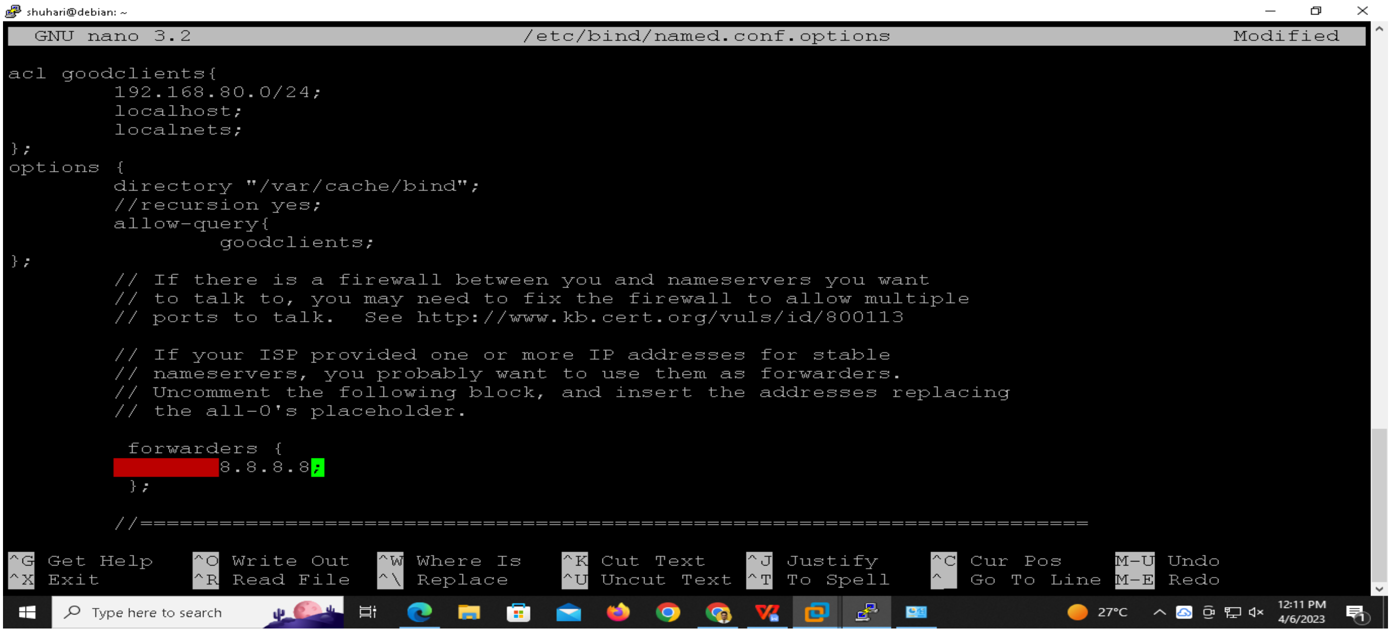
Answer should be non -authorative ./server : DNS server /address: 8.8.8.8

===

Forwarding

$ sudo nano /etc/bind/named.conf.options

(comment // recusrion and uncomment forwarders and add 8.8.8.8 inplace of 0.0.0.0

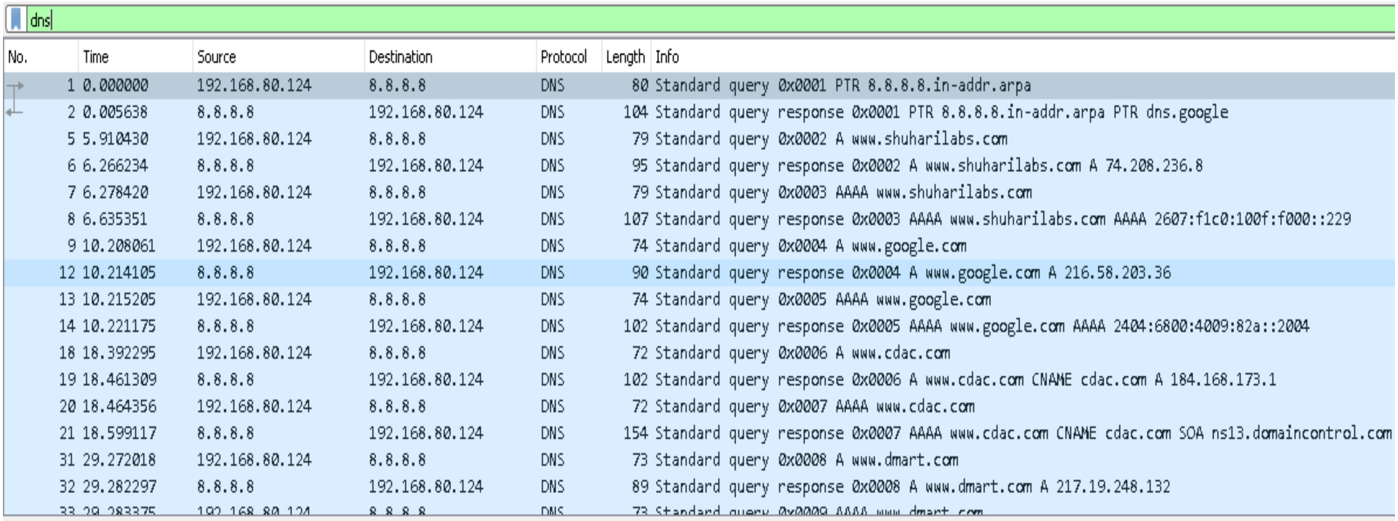


```
shuhari@debian: ~
  GNU nano 3.2                 /etc/bind/named.conf.options                 Modified

acl goodclients{
        192.168.80.0/24;
        localhost;
        localnets;
};
options {
        directory "/var/cache/bind";
        //recursion yes;
        allow-query{
                goodclients;
};
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
        [redacted]8.8.8.8;
         };

        //========================================================================

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos     M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^  Go To Line  M-E Redo
```

All steps remain same as mentioned above.

Packet Capturing.
$sudo apt-get install tcpdump
$sudo tcpdump -w dns.pcap (it will capture packets keep it on)

Go to VM windows ->win+r->ncpa.cpl->preferred dns server 8.8.8.8->cmd >nslookup>www.xyz.com
Winscp->insert ip where dns is configured->transfer pcap file to window ->open it with wireshark.
Result:

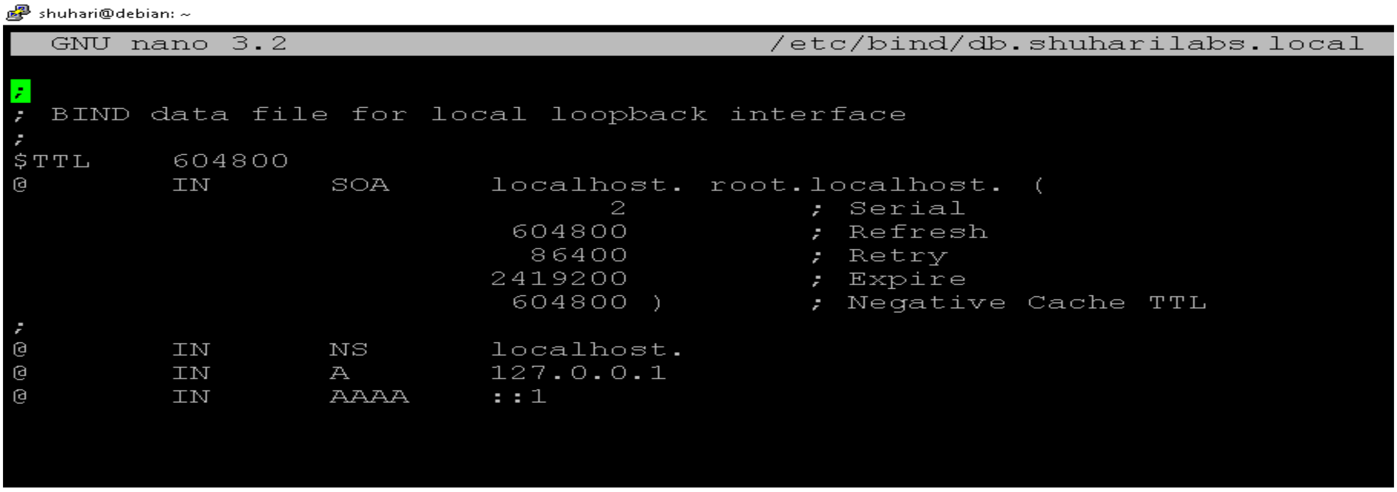


dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.124	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
2	0.005638	8.8.8.8	192.168.80.124	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
5	5.910430	192.168.80.124	8.8.8.8	DNS	79	Standard query 0x0002 A www.shuharilabs.com
6	6.266234	8.8.8.8	192.168.80.124	DNS	95	Standard query response 0x0002 A www.shuharilabs.com A 74.208.236.8
7	6.278420	192.168.80.124	8.8.8.8	DNS	79	Standard query 0x0003 AAAA www.shuharilabs.com
8	6.635351	8.8.8.8	192.168.80.124	DNS	107	Standard query response 0x0003 AAAA www.shuharilabs.com AAAA 2607:f1c0:100f:f000::229
9	10.208061	192.168.80.124	8.8.8.8	DNS	74	Standard query 0x0004 A www.google.com
12	10.214105	8.8.8.8	192.168.80.124	DNS	90	Standard query response 0x0004 A www.google.com A 216.58.203.36
13	10.215205	192.168.80.124	8.8.8.8	DNS	74	Standard query 0x0005 AAAA www.google.com
14	10.221175	8.8.8.8	192.168.80.124	DNS	102	Standard query response 0x0005 AAAA www.google.com AAAA 2404:6800:4009:82a::2004
18	18.392295	192.168.80.124	8.8.8.8	DNS	72	Standard query 0x0006 A www.cdac.com
19	18.461309	8.8.8.8	192.168.80.124	DNS	102	Standard query response 0x0006 A www.cdac.com CNAME cdac.com A 184.168.173.1
20	18.464356	192.168.80.124	8.8.8.8	DNS	72	Standard query 0x0007 AAAA www.cdac.com
21	18.599117	8.8.8.8	192.168.80.124	DNS	154	Standard query response 0x0007 AAAA www.cdac.com CNAME cdac.com SOA ns13.domaincontrol.com
31	29.272018	192.168.80.124	8.8.8.8	DNS	73	Standard query 0x0008 A www.dmart.com
32	29.282297	8.8.8.8	192.168.80.124	DNS	89	Standard query response 0x0008 A www.dmart.com A 217.19.248.132
33	29.283375	192.168.80.124	8.8.8.8	DNS	73	Standard query 0x0009 AAAA www.dmart.com

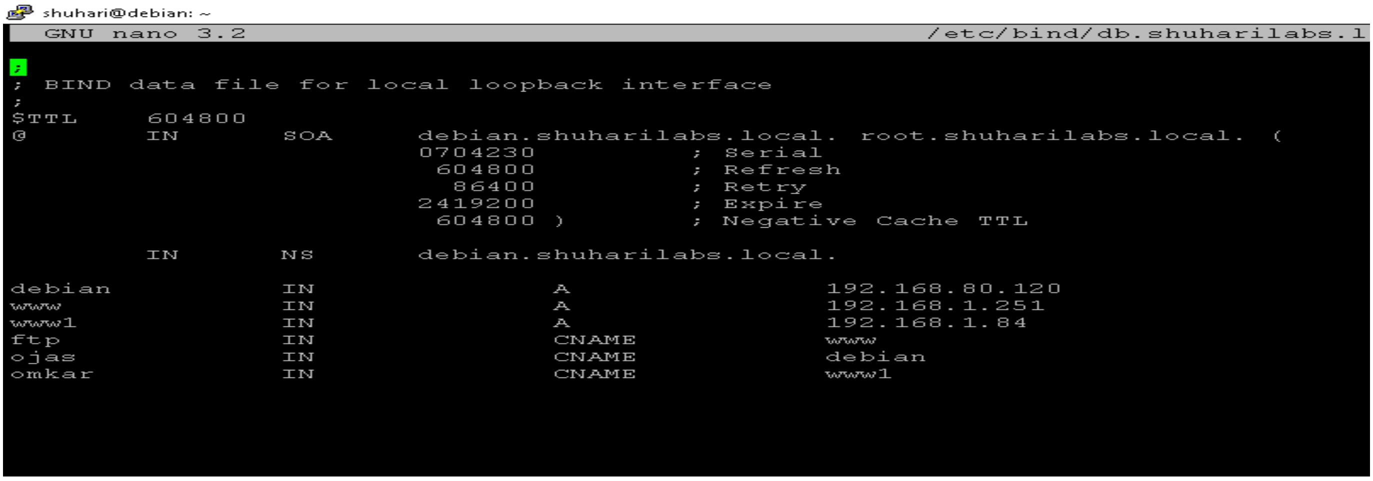
===
$sudo cp /etc/bind/db.local /etc/bind/db.shuharilabs.local (creating a copy of config file)

Before configuration:

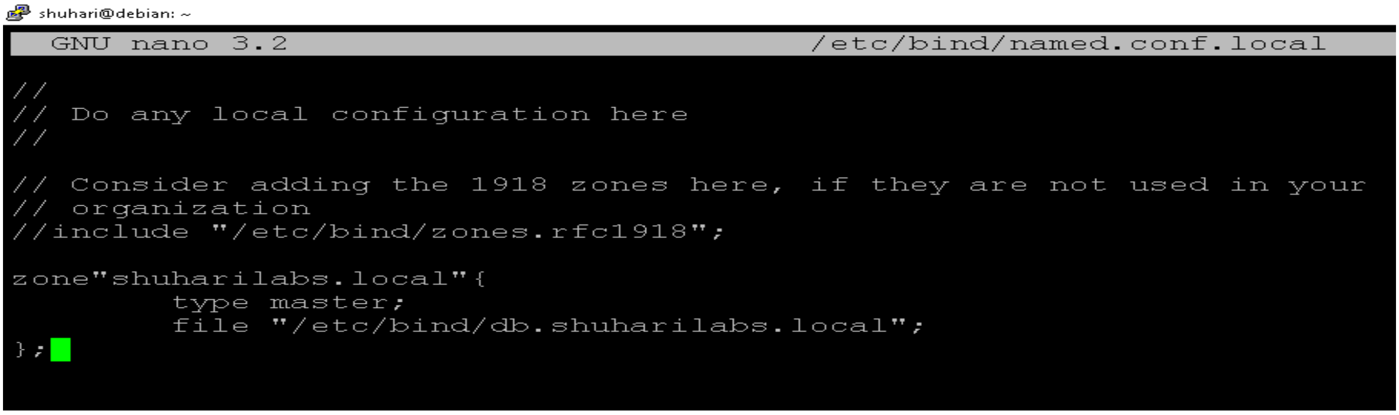


```
shuhari@debian: ~
  GNU nano 3.2                                /etc/bind/db.shuharilabs.local

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

After Configuration:
$sudo nano /etc/bind/named.conf.local



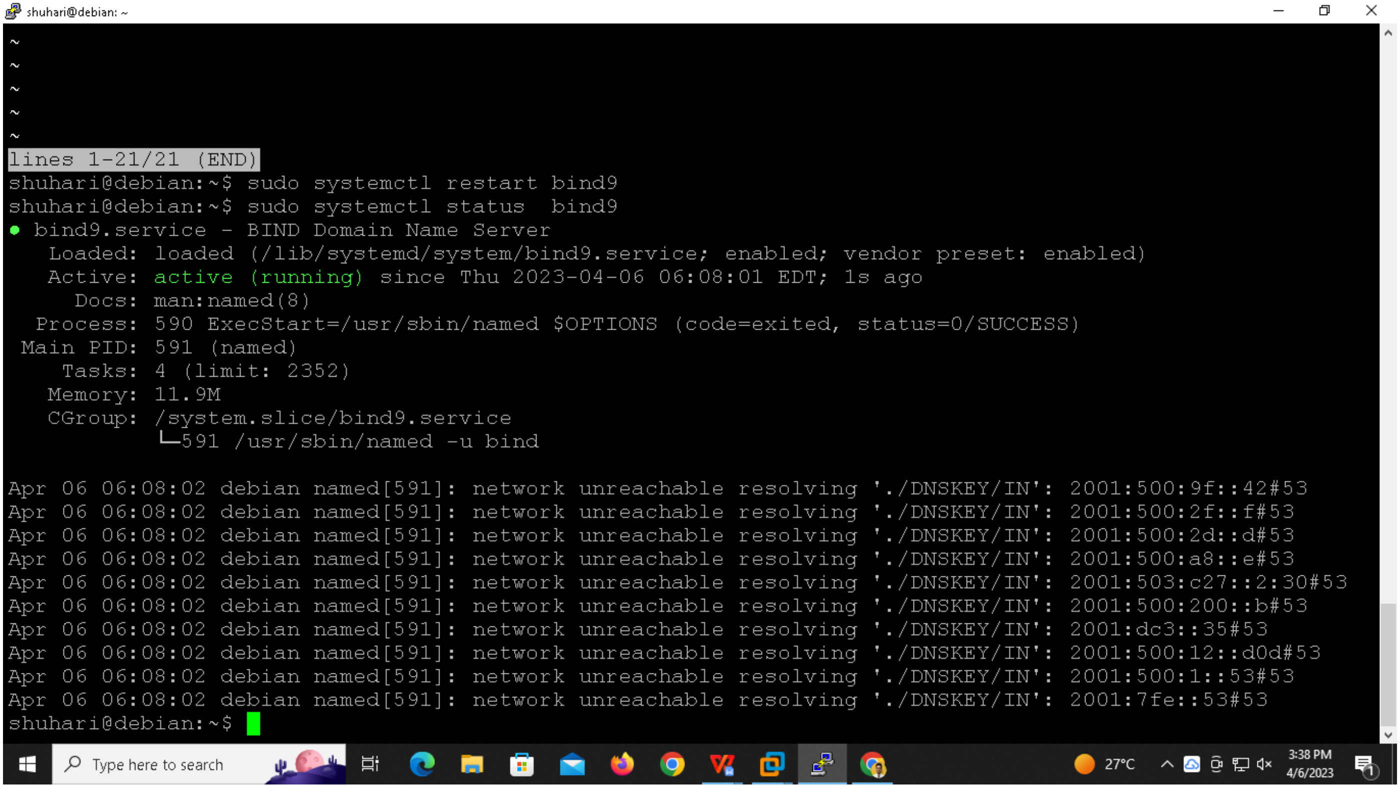
```
shuhari@debian: ~
  GNU nano 3.2                                               /etc/bind/db.shuharilabs.l

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.shuharilabs.local. root.shuharilabs.local. (
                        0704230         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

        IN      NS      debian.shuharilabs.local.

debian          IN              A               192.168.80.120
www             IN              A               192.168.1.251
www1            IN              A               192.168.1.84
ftp             IN              CNAME           www
ojas            IN              CNAME           debian
omkar           IN              CNAME           www1
```



```
shuhari@debian: ~
  GNU nano 3.2                    /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone"shuharilabs.local"{
        type master;
        file "/etc/bind/db.shuharilabs.local";
};
```

$ sudo systemctl restart bind9

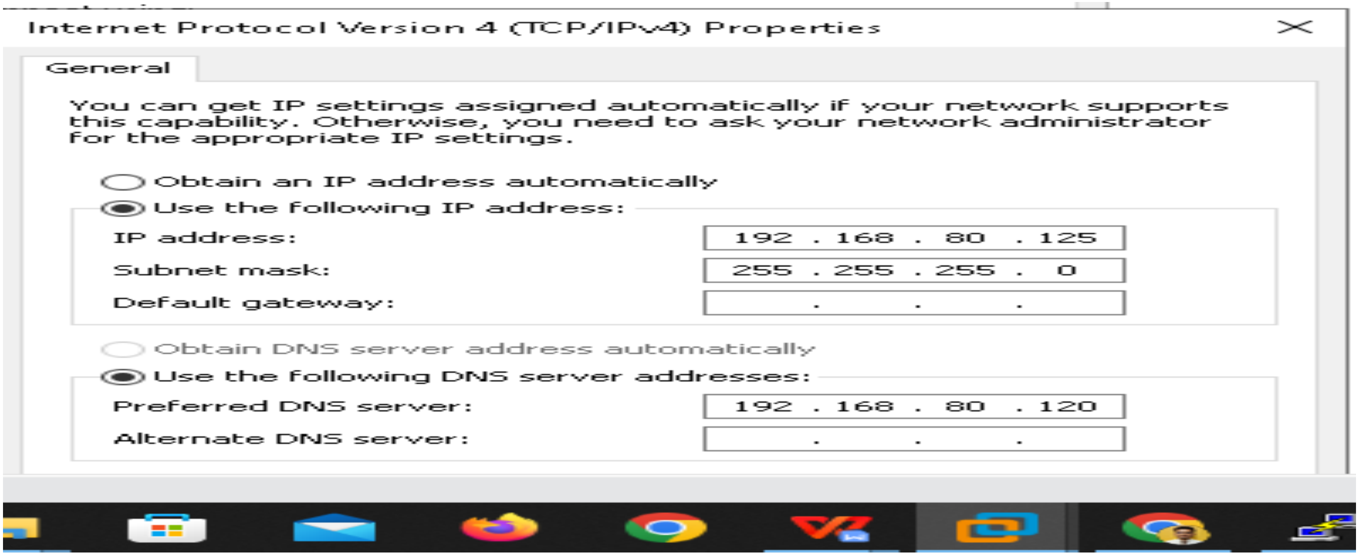
$ sudo system status bind9 (active:running)



```
shuhari@debian: ~
~
~
~
~
~
lines 1-21/21 (END)
shuhari@debian:~$ sudo systemctl restart bind9
shuhari@debian:~$ sudo systemctl status  bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-04-06 06:08:01 EDT; 1s ago
     Docs: man:named(8)
  Process: 590 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 591 (named)
    Tasks: 4 (limit: 2352)
   Memory: 11.9M
   CGroup: /system.slice/bind9.service
           └─591 /usr/sbin/named -u bind

Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
Apr 06 06:08:02 debian named[591]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
shuhari@debian:~$
```

Testing:(it will be performed on VM windows)

Vm windows (win+r, ncpa.cpl, properties allot static ip and subnet mask and debian ip in preff dns ser)



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 80 . 125

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

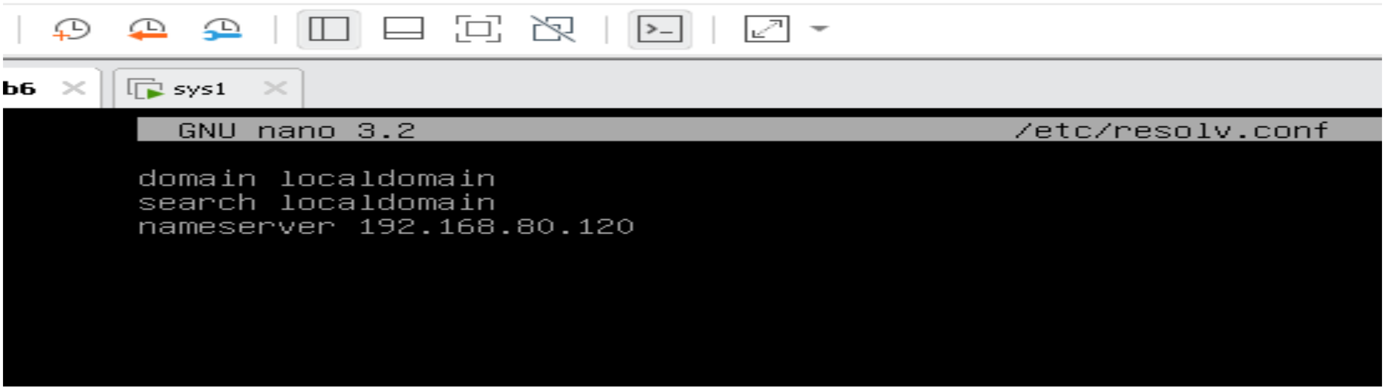
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 80 . 120

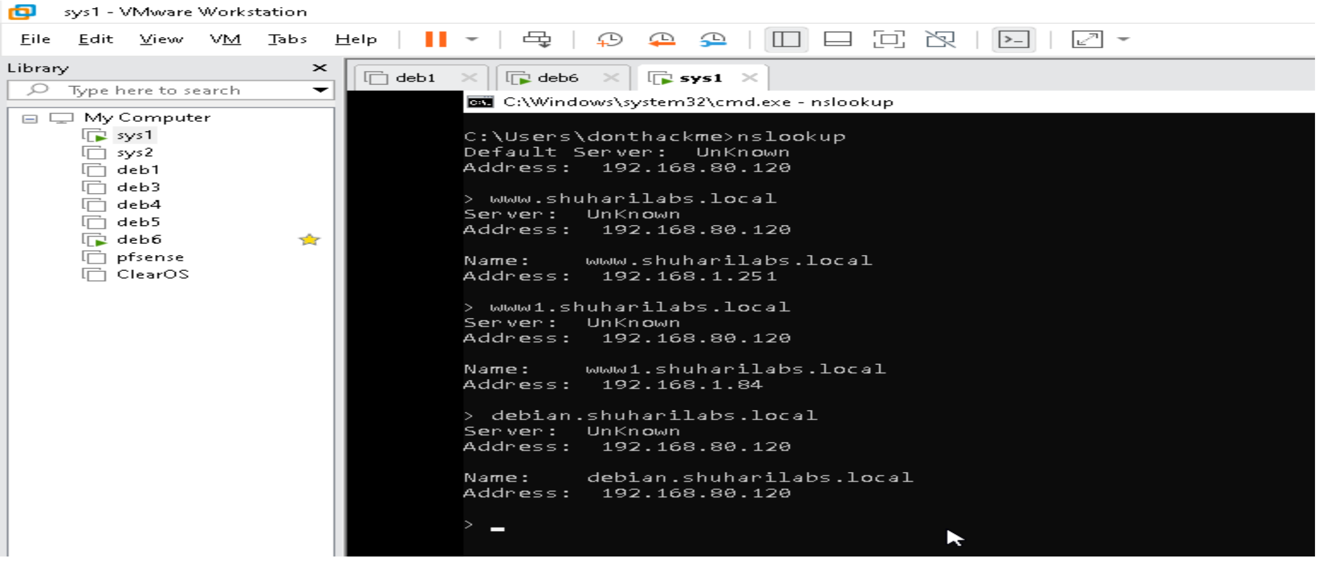
Alternate DNS server: . . .

$sudo nano /etc/resolv.conf -> instead of nameserver write IP of that debian.



```
GNU nano 3.2                                         /etc/resolv.conf

domain localdomain
search localdomain
nameserver 192.168.80.120
```

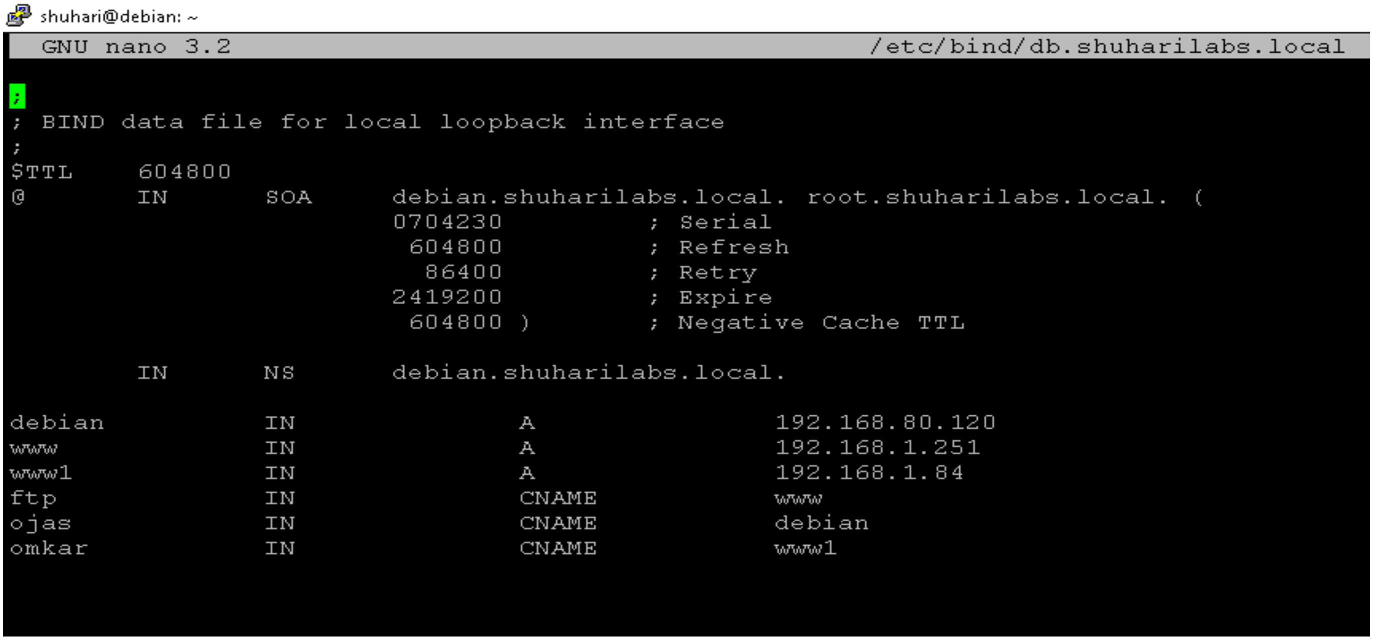
VM Windows ->cmd->nslookup->...



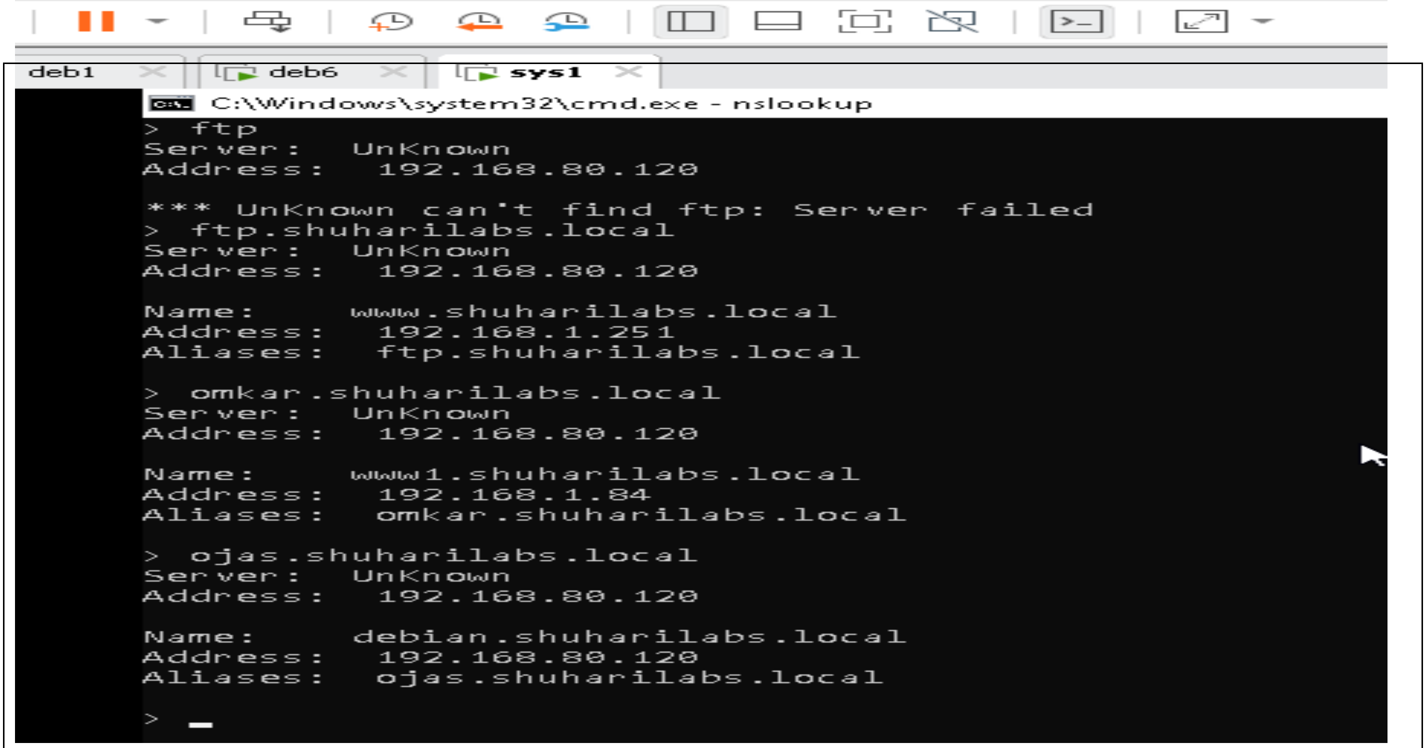
```
C:\Users\donthackme>nslookup
Default Server:  UnKnown
Address:  192.168.80.120

> www.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    www.shuharilabs.local
Address:  192.168.1.251

> www1.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    www1.shuharilabs.local
Address:  192.168.1.84

> debian.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    debian.shuharilabs.local
Address:  192.168.80.120

> _
```

==

Cname



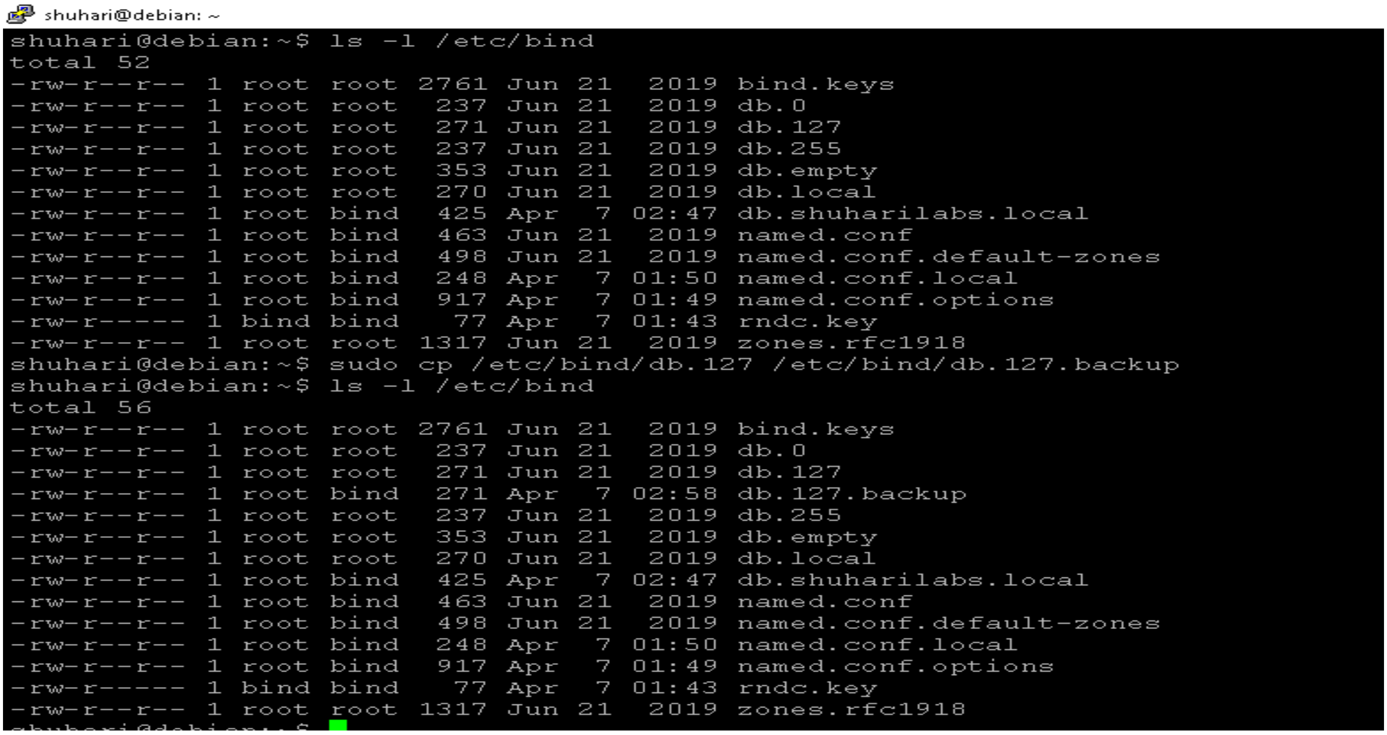
```
  GNU nano 3.2                                  /etc/bind/db.shuharilabs.local

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.shuharilabs.local. root.shuharilabs.local. (
                        0704230         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

        IN      NS      debian.shuharilabs.local.

debian          IN              A               192.168.80.120
www             IN              A               192.168.1.251
www1            IN              A               192.168.1.84
ftp             IN              CNAME           www
ojas            IN              CNAME           debian
omkar           IN              CNAME           www1
```



```
> ftp
Server:  UnKnown
Address:  192.168.80.120

*** UnKnown can't find ftp: Server failed
> ftp.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    www.shuharilabs.local
Address:  192.168.1.251
Aliases:  ftp.shuharilabs.local

> omkar.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    www1.shuharilabs.local
Address:  192.168.1.84
Aliases:  omkar.shuharilabs.local

> ojas.shuharilabs.local
Server:  UnKnown
Address:  192.168.80.120

Name:    debian.shuharilabs.local
Address:  192.168.80.120
Aliases:  ojas.shuharilabs.local

> _
```

Reverse lookup (IP ---> name)

$sudo cp /etc/bind/db.127 /etc/bind/db.127.backup (db.127 is file to allow server to search name for an IP)



```
shuhari@debian:~$ ls -l /etc/bind
total 52
-rw-r--r-- 1 root root 2761 Jun 21  2019 bind.keys
-rw-r--r-- 1 root root  237 Jun 21  2019 db.0
-rw-r--r-- 1 root root  271 Jun 21  2019 db.127
-rw-r--r-- 1 root root  237 Jun 21  2019 db.255
-rw-r--r-- 1 root root  353 Jun 21  2019 db.empty
-rw-r--r-- 1 root root  270 Jun 21  2019 db.local
-rw-r--r-- 1 root bind  425 Apr  7 02:47 db.shuharilabs.local
-rw-r--r-- 1 root bind  463 Jun 21  2019 named.conf
-rw-r--r-- 1 root bind  498 Jun 21  2019 named.conf.default-zones
-rw-r--r-- 1 root bind  248 Apr  7 01:50 named.conf.local
-rw-r--r-- 1 root bind  917 Apr  7 01:49 named.conf.options
-rw-r----- 1 bind bind   77 Apr  7 01:43 rndc.key
-rw-r--r-- 1 root root 1317 Jun 21  2019 zones.rfc1918
shuhari@debian:~$ sudo cp /etc/bind/db.127 /etc/bind/db.127.backup
shuhari@debian:~$ ls -l /etc/bind
total 56
-rw-r--r-- 1 root root 2761 Jun 21  2019 bind.keys
-rw-r--r-- 1 root root  237 Jun 21  2019 db.0
-rw-r--r-- 1 root root  271 Jun 21  2019 db.127
-rw-r--r-- 1 root bind  271 Apr  7 02:58 db.127.backup
-rw-r--r-- 1 root root  237 Jun 21  2019 db.255
-rw-r--r-- 1 root root  353 Jun 21  2019 db.empty
-rw-r--r-- 1 root root  270 Jun 21  2019 db.local
-rw-r--r-- 1 root bind  425 Apr  7 02:47 db.shuharilabs.local
-rw-r--r-- 1 root bind  463 Jun 21  2019 named.conf
-rw-r--r-- 1 root bind  498 Jun 21  2019 named.conf.default-zones
-rw-r--r-- 1 root bind  248 Apr  7 01:50 named.conf.local
-rw-r--r-- 1 root bind  917 Apr  7 01:49 named.conf.options
-rw-r----- 1 bind bind   77 Apr  7 01:43 rndc.key
-rw-r--r-- 1 root root 1317 Jun 21  2019 zones.rfc1918
shuhari@debian:~$
```

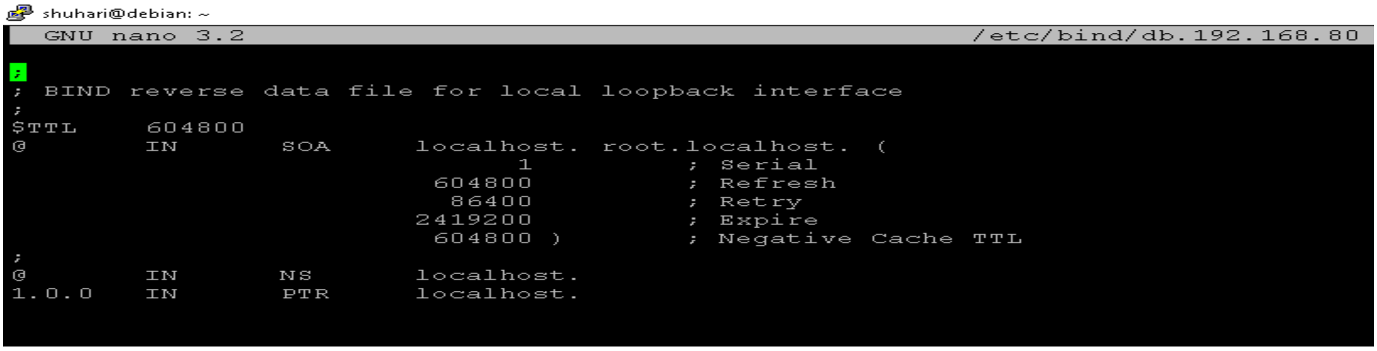
1)Creating a new file with our IP name till three places.(db.192.168.80)

$sudo cp /etc/bind/db.127 /etc/bind/db.192.168.80

2)Edit the configuration file

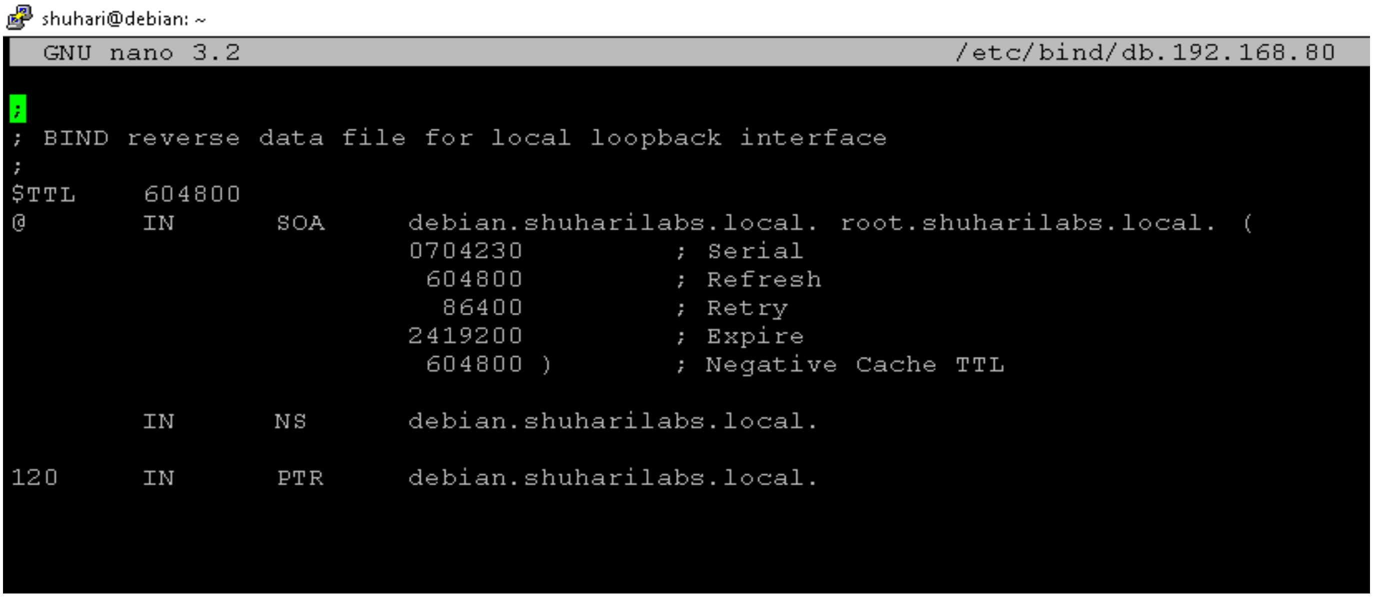
$sudo nano /etc/bind/db.192.168.80

Before Config



```
  GNU nano 3.2                                        /etc/bind/db.192.168.80

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

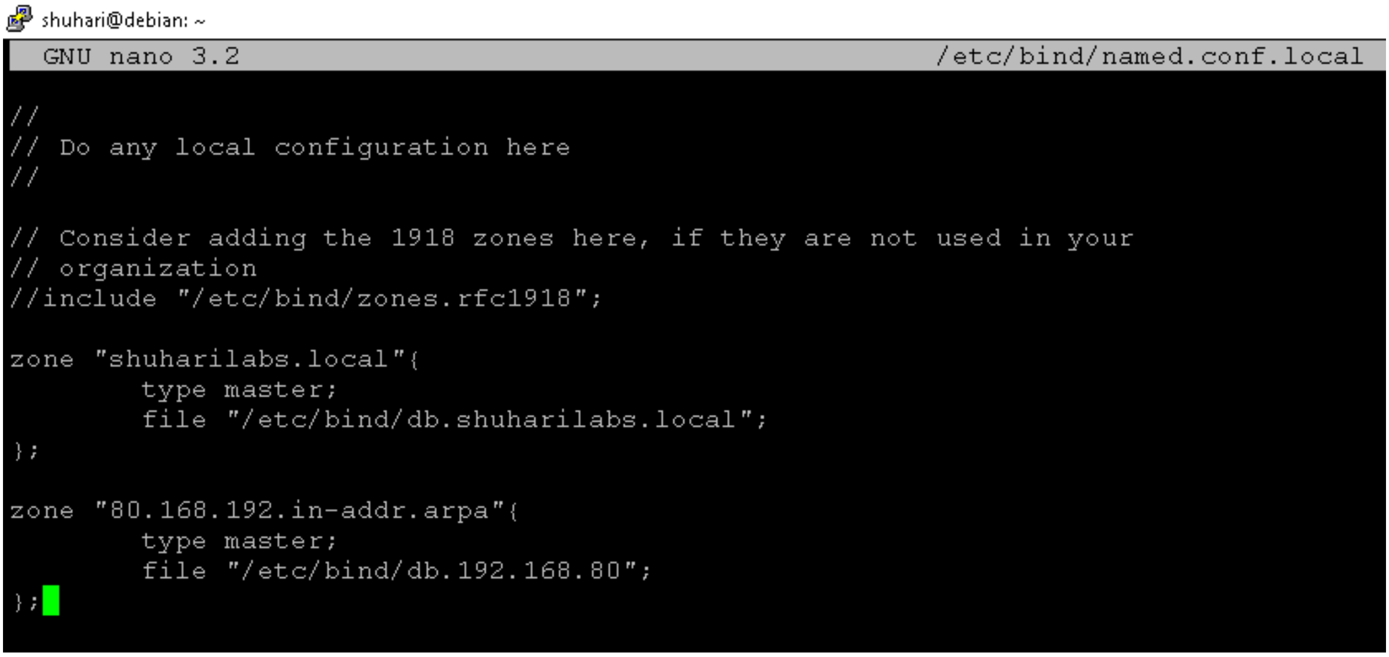
After configuration .



```
  GNU nano 3.2                                        /etc/bind/db.192.168.80

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.shuharilabs.local. root.shuharilabs.local. (
                        0704230         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

        IN      NS      debian.shuharilabs.local.

120     IN      PTR     debian.shuharilabs.local.
```

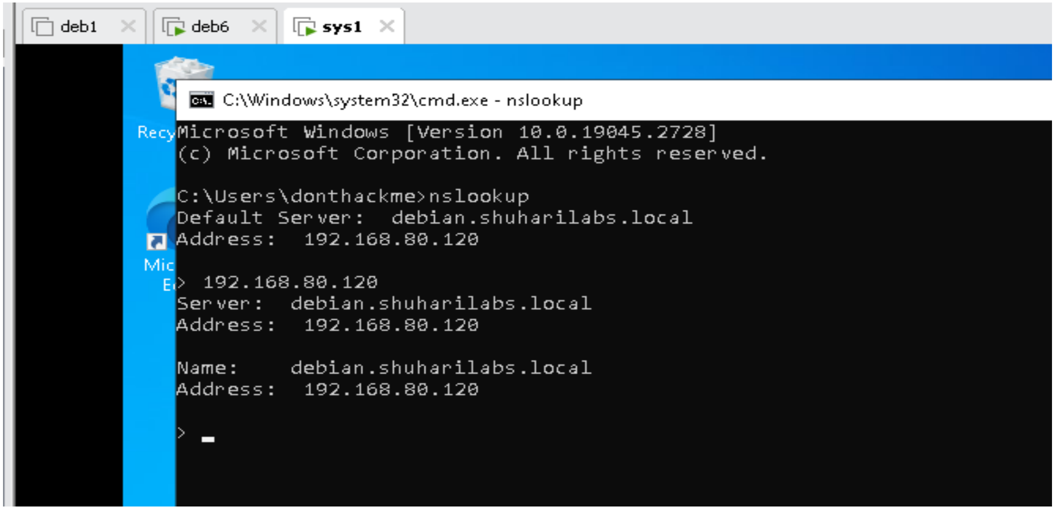
Editing the config file

$sudo nano /etc/bind/named.conf.local (add zone for IP to name)



```
  GNU nano 3.2                                        /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "shuharilabs.local"{
        type master;
        file "/etc/bind/db.shuharilabs.local";
};

zone "80.168.192.in-addr.arpa"{
        type master;
        file "/etc/bind/db.192.168.80";
};
```

Testing:(Vm windows -> win r->cmd)



```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\donthackme>nslookup
Default Server:  debian.shuharilabs.local
Address:  192.168.80.120

> 192.168.80.120
Server:  debian.shuharilabs.local
Address:  192.168.80.120

Name:    debian.shuharilabs.local
Address:  192.168.80.120

> _
```

Omkar Ojas

Digitally signed by Omkar Ojas
Date: 2023.04.08 20:07:33 +05'30'