DNS Setup

Sudo apt-get update

Sudo apt-get upgrade

Sudo apt-get dist-upgrade

Install Bind9

Sudo apt-get install bind9 bind9utils bind9-doc

Sudo service bind9 start

START SERVICE AND ONLY RESTART AFTER DOING THE CHECK CMD

Add domain to host file

Sudo vi /etc/hosts

eth0ip #hostname.free.dom #sometimes interfaces is called enp0s3

127.0.0.1 localhost

127.0.0.1 <hostname>

Save & Exit

@ is the Server name

masterdns is the server name

secondarydns is the server name

every mention of these has to be changed to the proper machine

free.dom is the domain name

this should be changed to our domain “git.gud”

give the zone files a db.something so red team does not immediately know the forward and reverse files

Create Forward Zone files

Sudo vi /etc/bind/forward.free

$TTL 604800

@ IN SOA masterdns.free.dom root.free.dom (

101010 ;Serial

36000 ;Refresh

1800 ;Retry

604800 ;Expire

86400 ;Minimum TTL

)

@ IN NS masterdns.free.dom.

@ IN NS secondarydns.free.dom.

@ IN NS 10 mail.example.com.

Mail IN A Mail address

masterdns IN A 172.20.241.27

secondarydns IN A 172.20.240.25

--------------------------------------------------------------------------------------------------------------------------------------------

Create Reverse Zone

Sudo vi /etc/bind/reverse.free

--------------------------------------------------------------------------------------------------------------------------------------------

$TTL 604800

@ IN SOA masterdns.free.dom. root. Free.dom. (

101010 ;Serial

3600 ;Refresh

1800 ;Retry

604800 ;Expire

86400 ;Minimum TTL

)

@ IN NS masterdns.free.dom.

@ IN NS secondarydns.free.dom.

@ IN MX 10 mail.example.com.

Mail IN A mail address

Masterdns IN A 172.20.241.27

Secondarydns IN A 172.20.240.25

101 IN PTR masterdns.free.dom.

102 IN PTR secondarydns.free.dom.

--------------------------------------------------------------------------------------------------------------------------------------------

(may have to replace masterdns with secondary dns )

Define forward and reverse files

Sudo vi /etc/bind/named.conf.local

Zone “free.dom”{

Type master;

File “/etc/bind/forward.free”;

Allow-transfer {172.20.241.27;};

Also-notify {172.20.241.27;};

};

Zone “240.20.172.in-addr.arpa” {

Type master;

File “/etc/bind/reverse.free”;

Allow-transfer {172.20.241.27;};

Also-notify {172.20.241.27;};

};

logging {

channel query.log {

file "/var/lib/bind/query.log";

// Set the severity to dynamic to see all the debug messages.

severity debug 3;

};

category queries { query.log; };

};

Verify the DNS configuration files

Sudo named-checkconf /etc/bind/named.conf

Sudo named-checkconf /etc/bind/named.conf.local

Sudo named-checkzone free.dom /etc/bind/forward.free

Sudo named-checkzone free.dom /etc/bind/reverse.free

Restart and check bind9 service

Sudo systemctl restart bind9

Dig masterdns.free.dom

Service bind9 status

Add DNS server

Sudo vi /etc/network/interfaces

Auto eth0

Iface eth0 inet static

Address 172.168.1.101

Netmask 255.255.255.0

Network 172.168.1.0

Broadcast 172.168.1.255

Gateway 172.168.1..1

Dns-nameservers 172.168.1.101

Dns-search free.dom

Add Forwarders

vi /etc/bind/named.conf.options

acl hostname {

172.168.1.101;

localhost;

localnets;

};

options {

directory "/var/cache/bind";

recursion yes;

allow-query { hostname; };

forwarders {

8.8.8.8;

8.8.4.4;

};

forward only;

dnssec-enable yes;

watch out for this - it may shut everything down # dnssec-validation auto;

auth-nxdomain no; # conform to RFC1035

listen-on-v6 { any; };

};

Allow & Check DNS ports on the firewall

Sudo ufw enable

Sudo ufw status

Sudo ufw allow bind9

Sudo default deny outgoing

Sudo ufw allow 53

Move bind configs

Sudo mkdir –p /chroot/named

Sudo cp /etc/bind/named.conf /chroot/named/named.conf

Sudo cp /etc/bind/named.conf.local /chroot/named/named.conf.local

Change masters in the chroot to slaves

Sudo vi /chroot/named/named.conf.local

--------------------------------------------------------------------------------------------------------------------------------------------

Zone”free.dom” {

Type slave;

File ‘/etc/bind/forward.free”;

Allow-transfer { 172.20.241.27;};

Also-notify { 172.20.241.27;};

};

Zone “240.20.172.inaddr.arpa” { #use last 3 octets of network

Type slave;

File “/etc/bind/reverse.free”;

Allow-transfer { 172.20.241.27;};

Also-notify { 172.20.241.27;};

};

Set the proper permissions and ownership to the bind9 directory

Sudo chmod 755 /chroot/named

Sudo chmod –R 755 /etc/bind

Sudo chown bind:bind /chroot/named

sudo chown bind:bind /etc/bind/

Sudo chown bind:bind /chroot/named/slave

Cd /chroot/named

Sudo mkdir –p /etc/namedb/slave var/run

Create the devices BIND9 requires

Sudo mkdir /chroot/named/dev

Sudo mknod /chroot/named/dev/null c 1 3

Sudo mknod /chroot/named/dev/random c 1 8

Give the user bind access

Sudo chown bind:bind /chroot/named/var/run

To test if you successfully chroot

Sudo su bind

Try to change anything in

Sudo vi /etc/default/bind9

--------------------------------------------------------------------------------------------------------------------------------------------

OPTIONS=’-u bind –t /chroot/named –c /etc/named.conf

--------------------------------------------------------------------------------------------------------------------------------------------

Sudo vi chroot/named/etc/named.conf

--------------------------------------------------------------------------------------------------------------------------------------------

Options {

Directory “/etc/namedb”;

Pid-file “/var/run/named.pid”;

Statistics-file “var/run/named.stats”;

};

--------------------------------------------------------------------------------------------------------------------------------------------