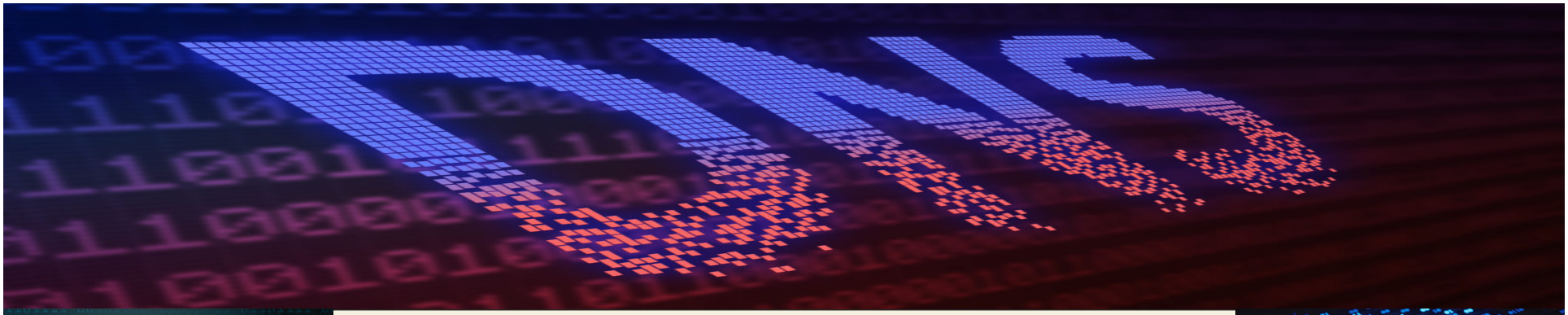


DNS Attacks

Sanjay Adiwal,
Principal Technical Officer
C-DAC Bengaluru

Contents

- Attacks on DNS Server
  - Attacks on DNS Infrastructure
  - Attacks exploiting the DNS Infrastructure
- DEMO
  - DNS Reflection/Amplification Attack
  - DNS Cache Poisoning Attack
  - DNS Tunneling Attack

Guess Who?

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

Guess Who?

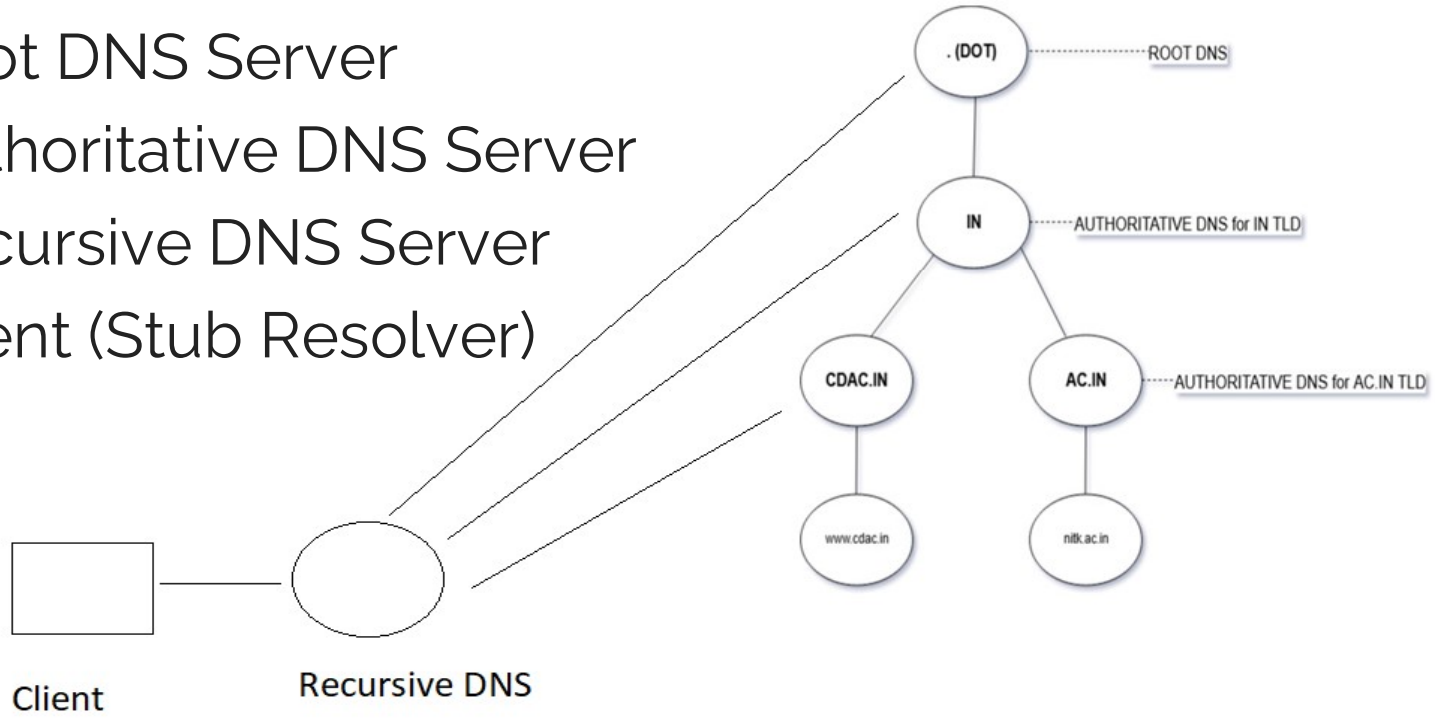
- Once one of the FBI's Most Wanted because he hacked into 40 major corporations just for the challenge .
- Kevin is now a trusted security consultant to the Fortune 500 and governments worldwide.

What is DNS?

- DNS is the most critical component of Internet Infrastructure.
- Service or Application that converts Domain names to IP Addresses:
  - www.nitk.ac.in. → DNS → 218.248.46.85
  - www.nitk.ac.in. → DNS → 2402:3a80:1fff:3f::d2d4:c204
- ... and back:
  - 218.248.46.85 → DNS → www.nitk.ac.in.
  - 2402:3a80:1fff:3f::d2d4:c204 → DNS → www.nitk.ac.in.

DNS Infrastructure

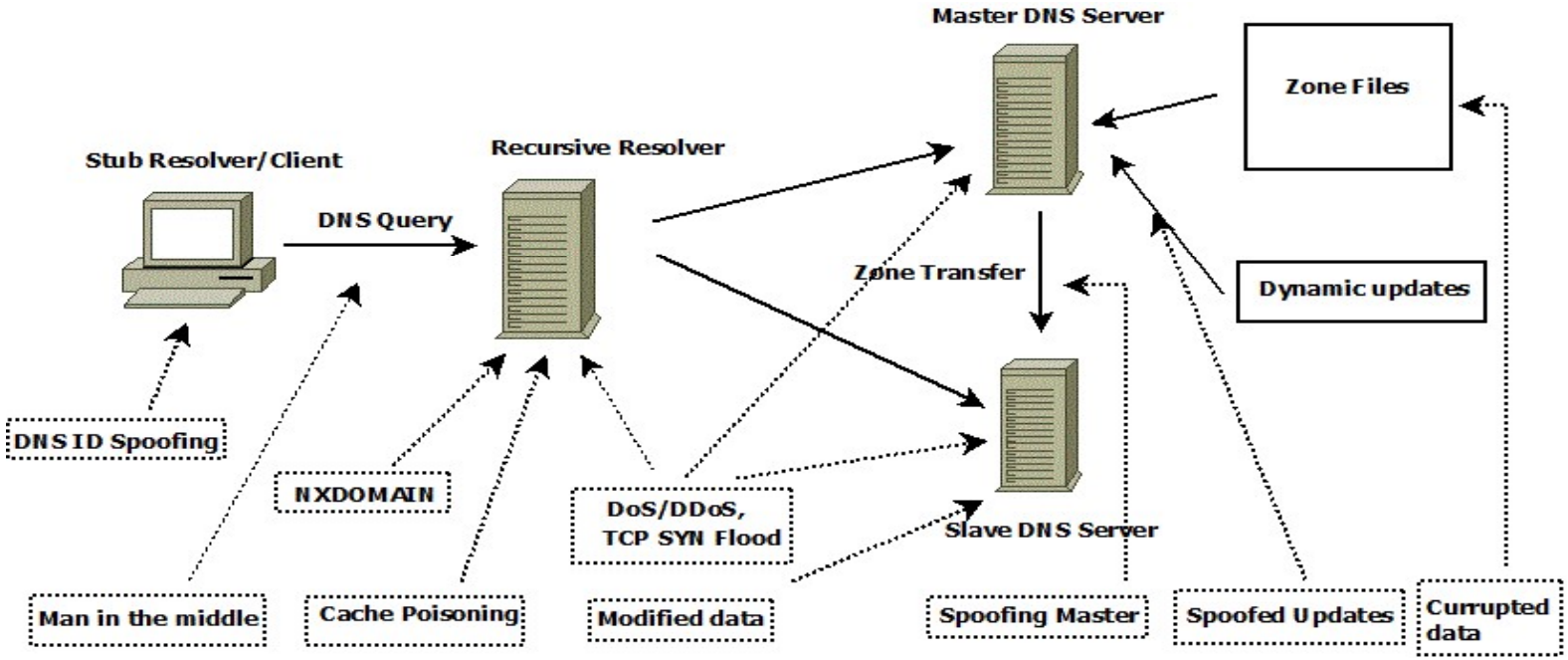
- Root DNS Server
- Authoritative DNS Server
- Recursive DNS Server
- Client (Stub Resolver)



DNS Attacks types

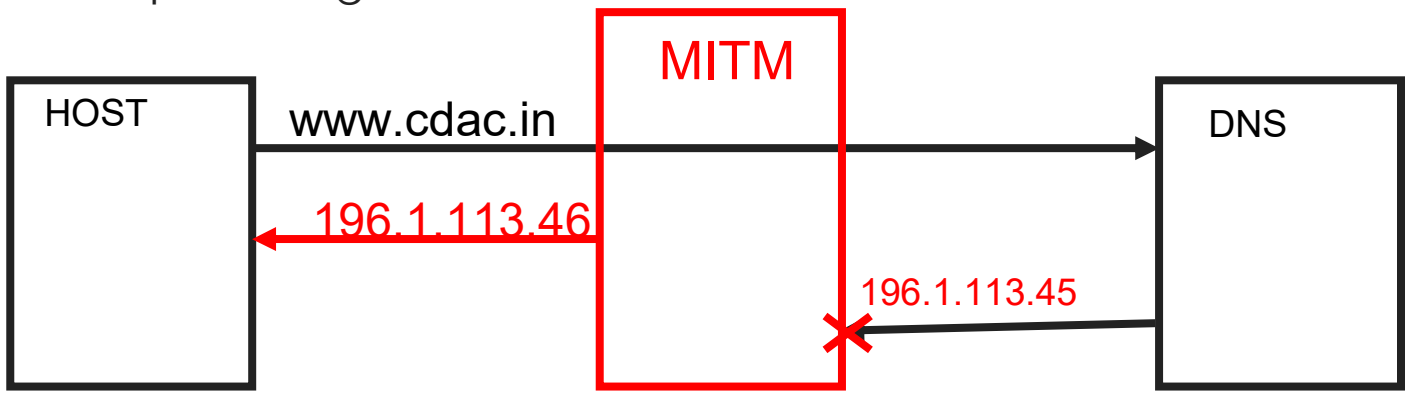
- Attacks on DNS Infrastructure
  - Attacks on Root, Authoritative and Recursive DNS, Stub resolver.
  - DoS/DDoS, DNS Cache Poisoning, DNS MITM etc.
- Attacks exploiting the DNS Infrastructure
  - Attacks on target system using DNS Infrastructure.
  - Reflection, Amplification, Tunnelling etc.

Attacks on DNS Infrastructure

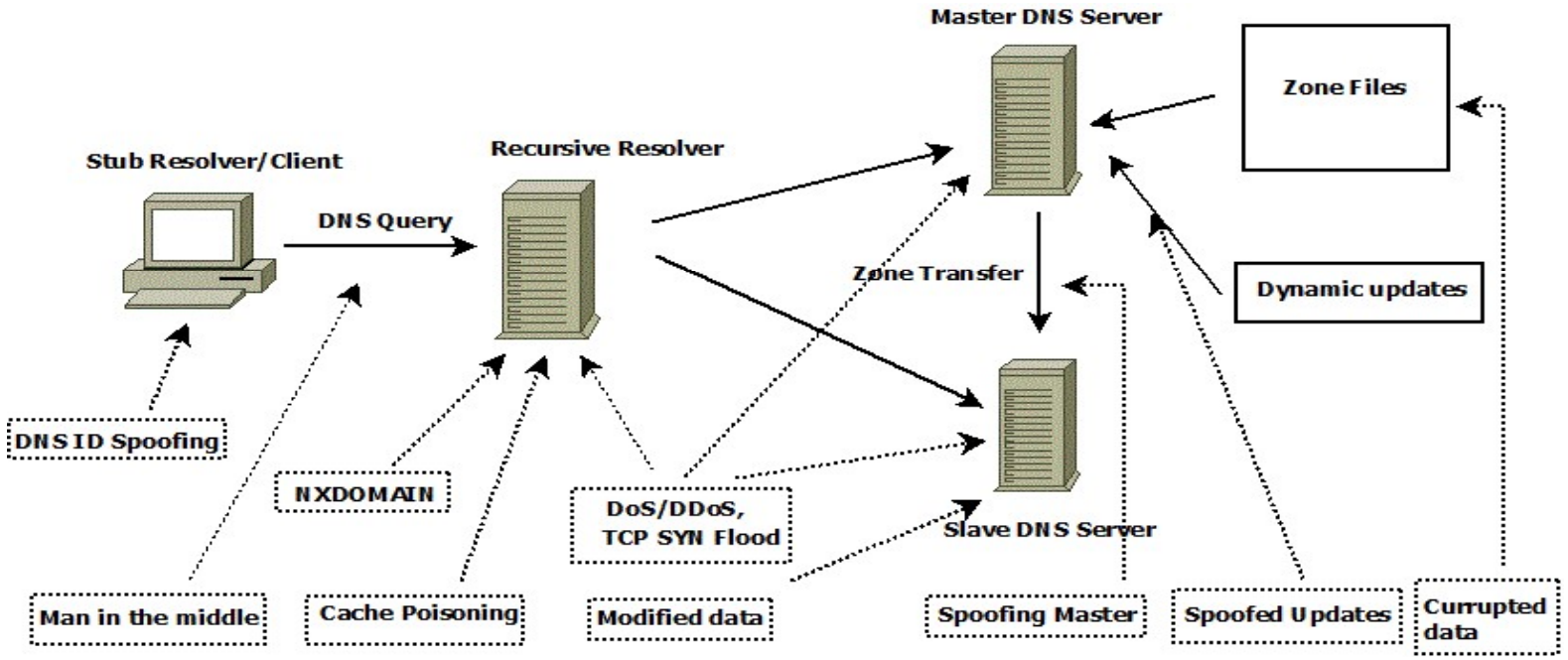


Man in The Middle Attack

- 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.
- ARP cache poisoning in LAN.

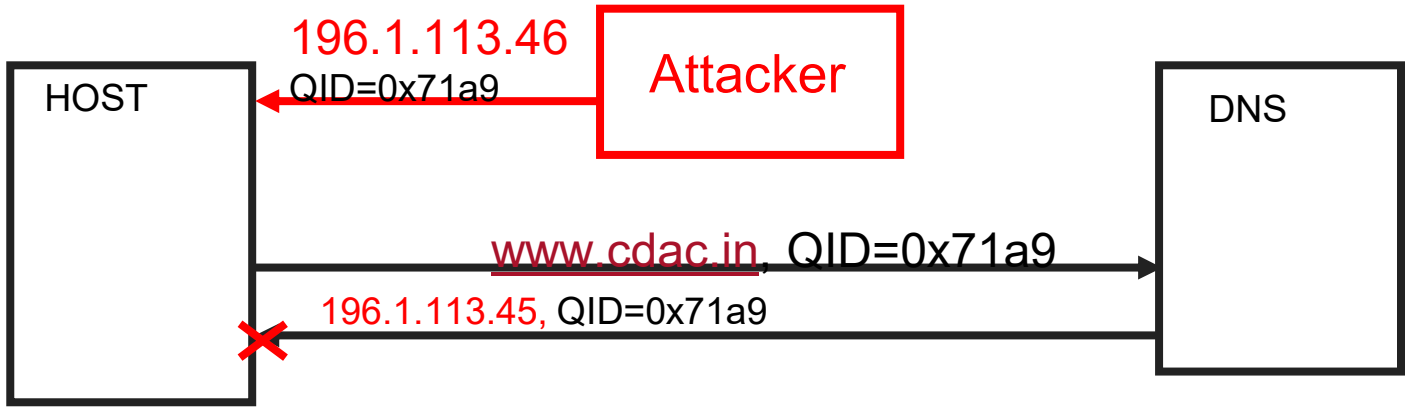


Attacks on DNS Infrastructure

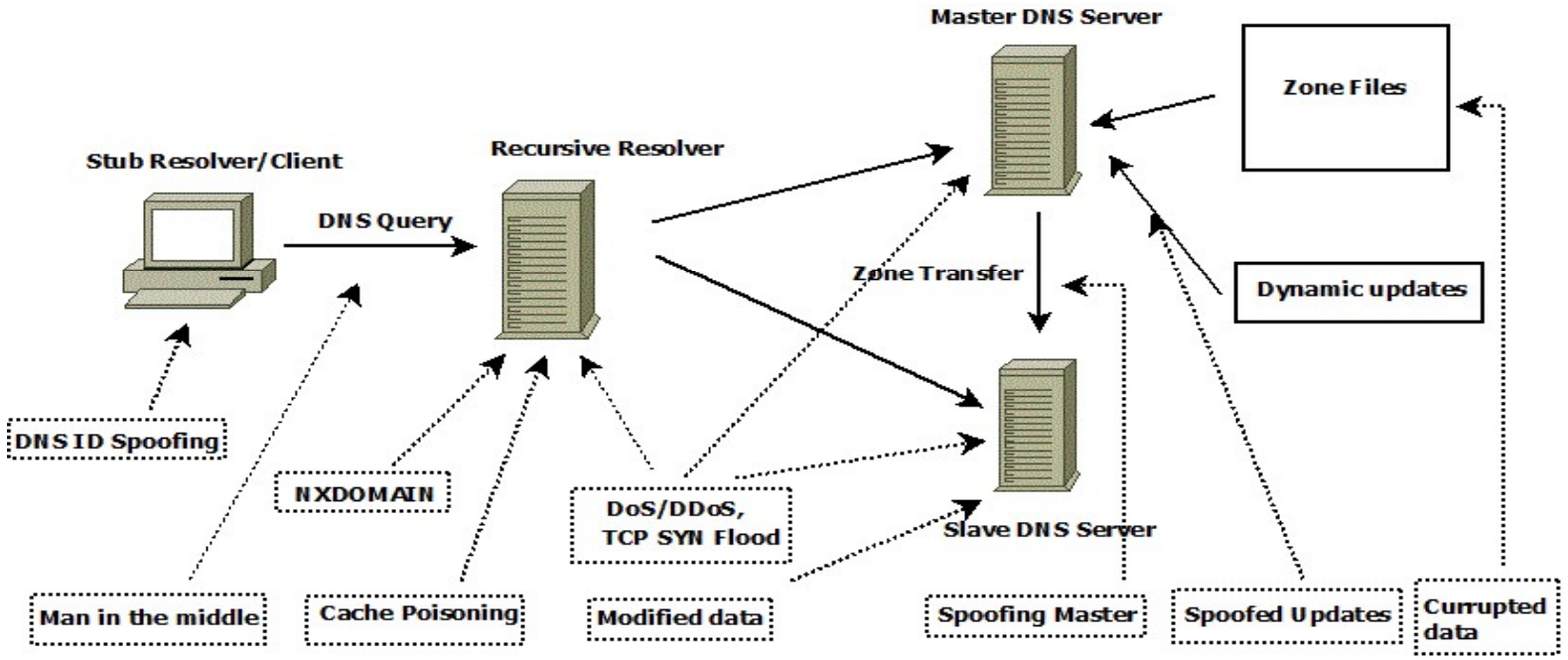


DNS ID Spoofing

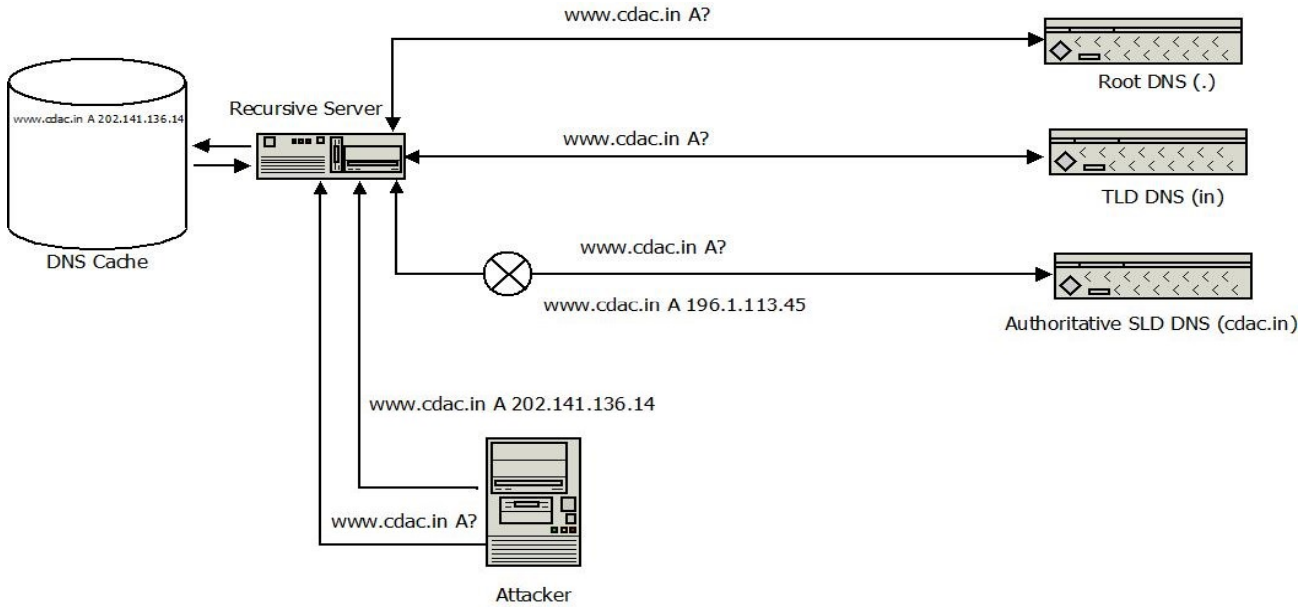
- DNS Client has query ID associated with each DNS query.
- If attacker knows the query ID, reply with fake records.



Attacks on DNS Infrastructure

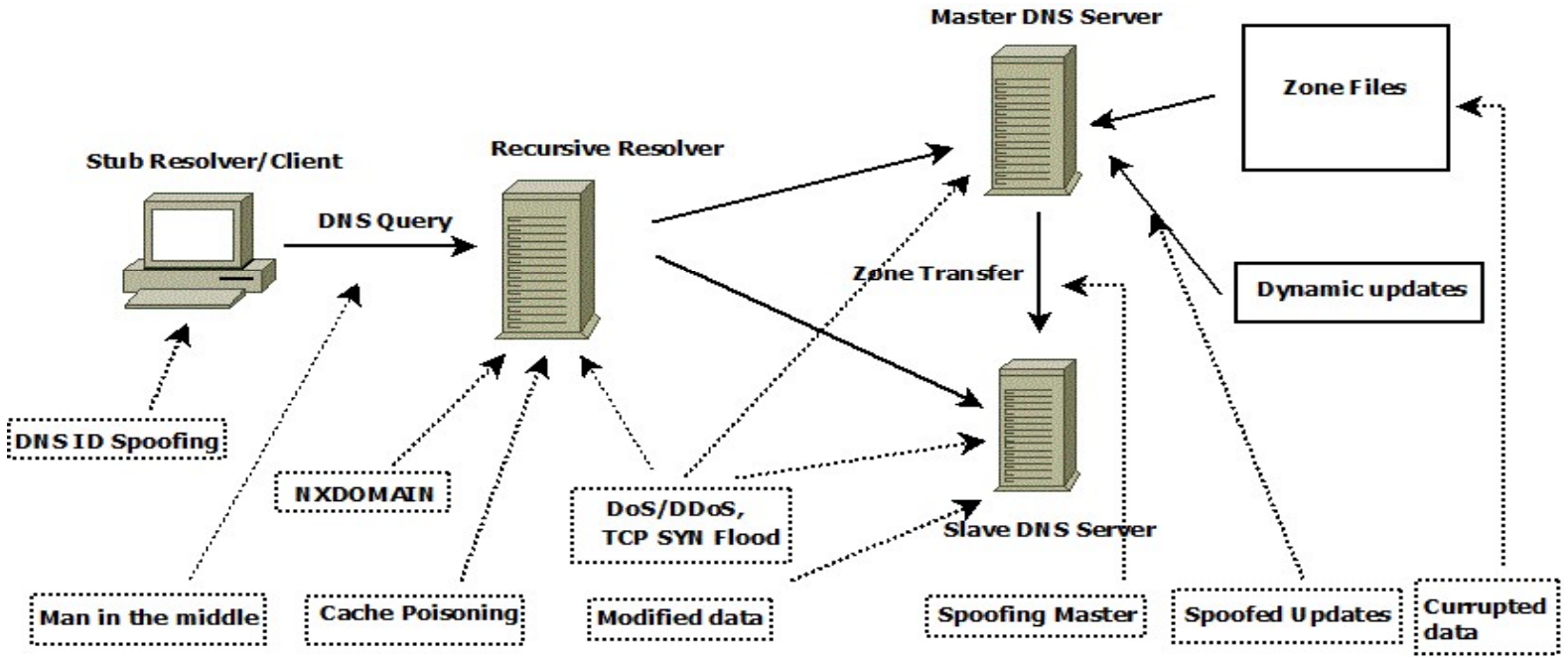


DNS Cache poisoning

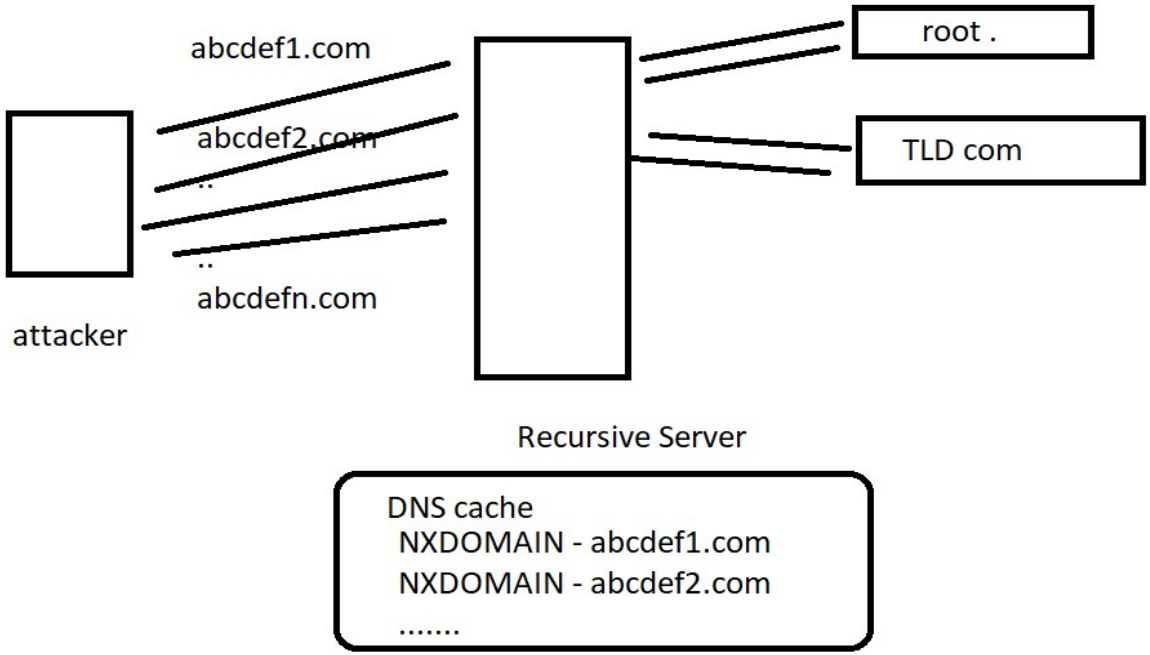


- DEMO

Attacks on DNS Infrastructure



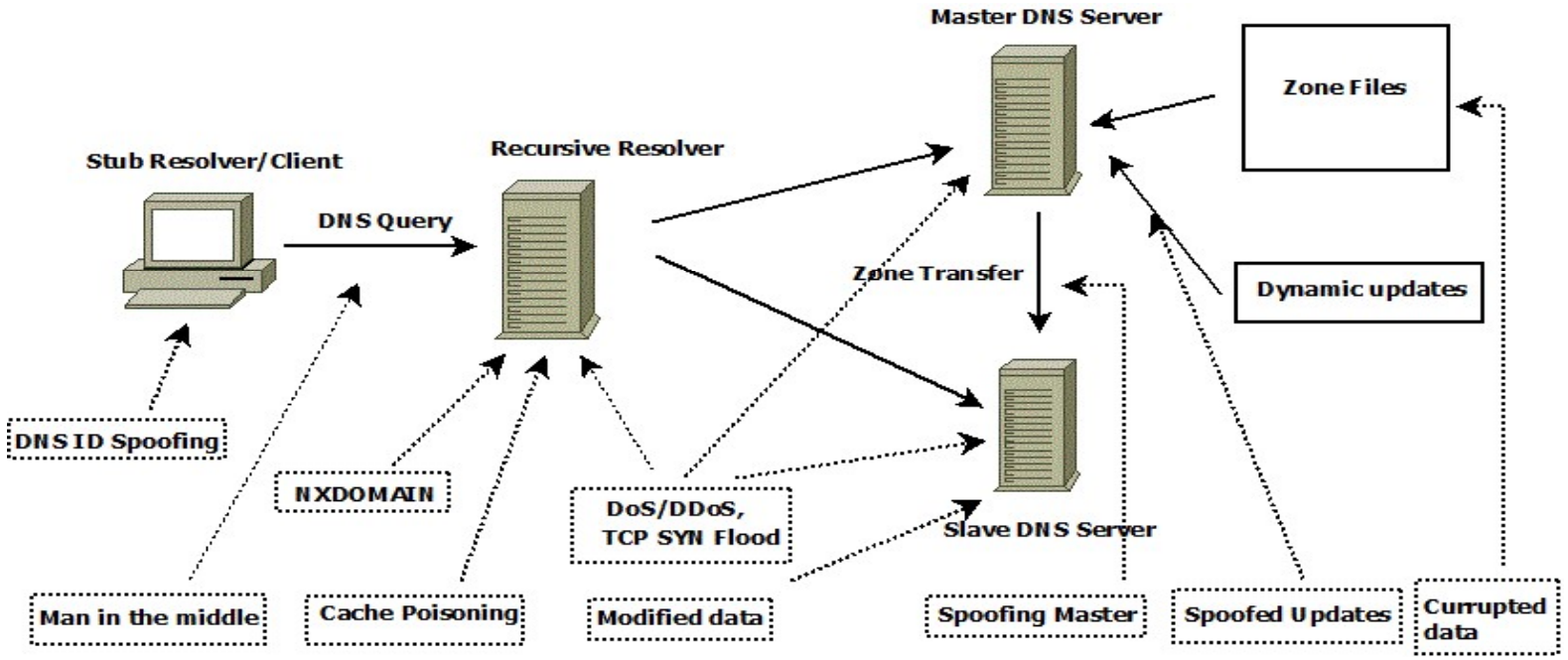
NXDOMAIN


abcdef1.com
abcdef2.com
..
..
abcdefn.com
attacker
root .
TLD com
Recursive Server
DNS cache
NXDOMAIN - abcdef1.com
NXDOMAIN - abcdef2.com
.....

NXDOMAIN

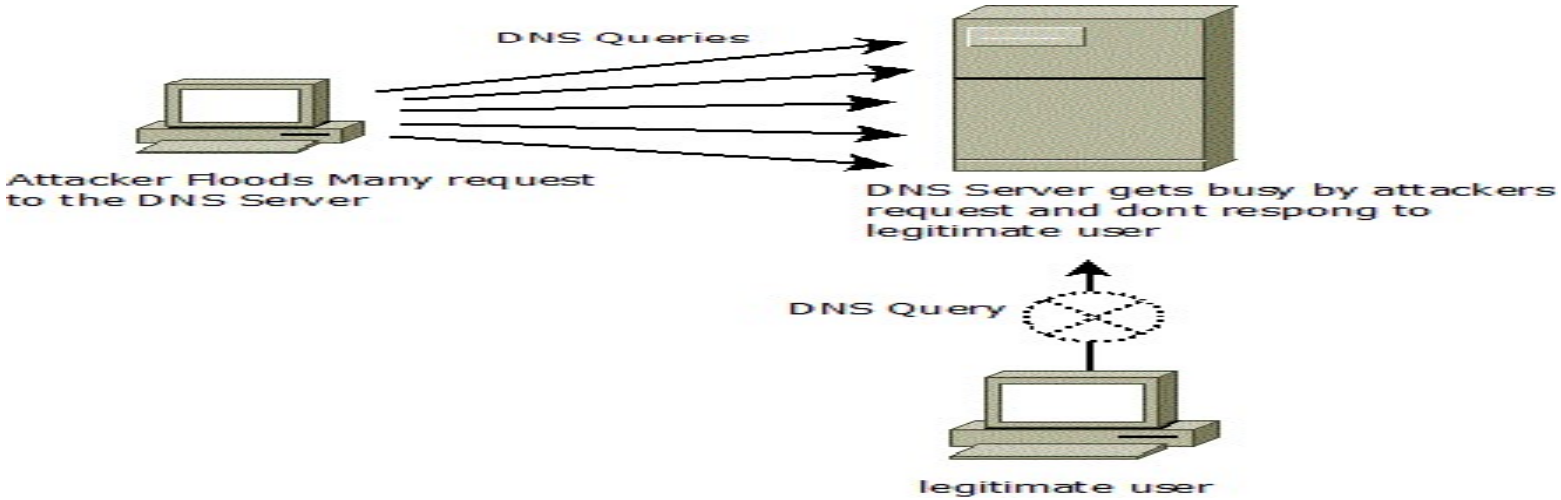
- The attacker sends the flood of queries to Recursive DNS server for resolving of non existing domain name.
- DNS Server cannot find the answer of the query and reply back with NXDOMAIN results, in process the recursive DNS servers cache data fills up with NXDOMAIN results, which slows down the response time for the legitimate user.
- If high volume flood of queries generated then cache fills up very quickly, and the legitimate user feels high delay for their responses.

Attacks on DNS Infrastructure



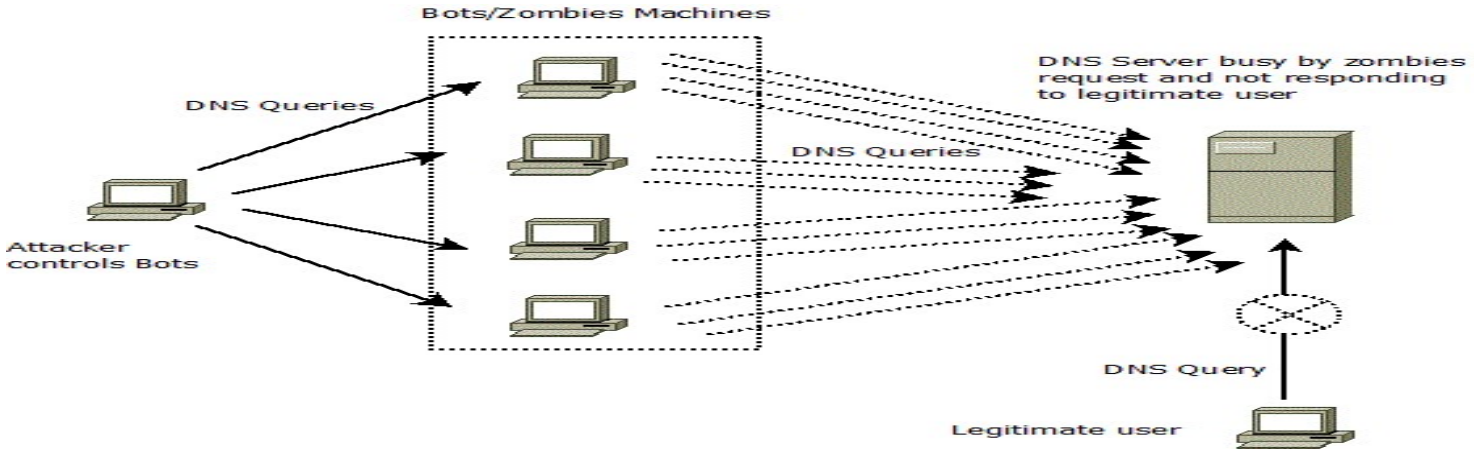
DoS

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

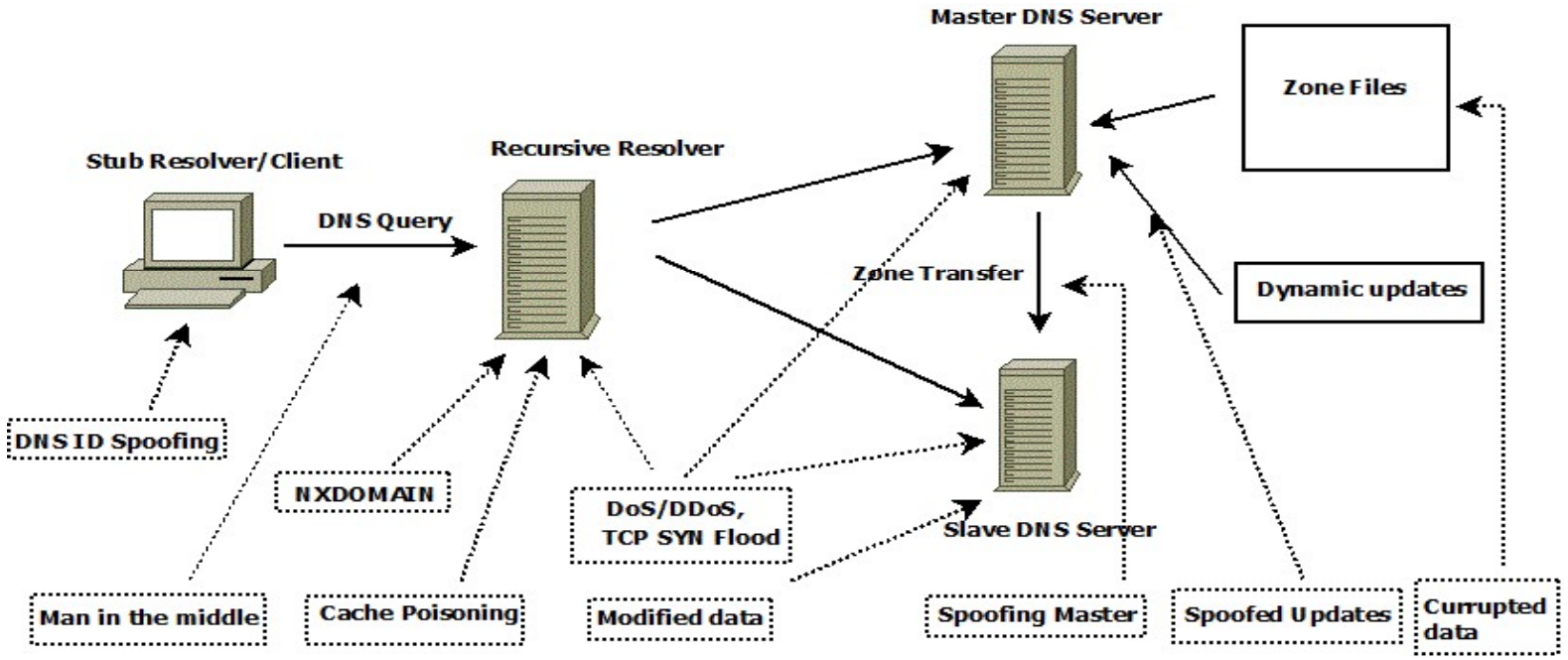


DDoS

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



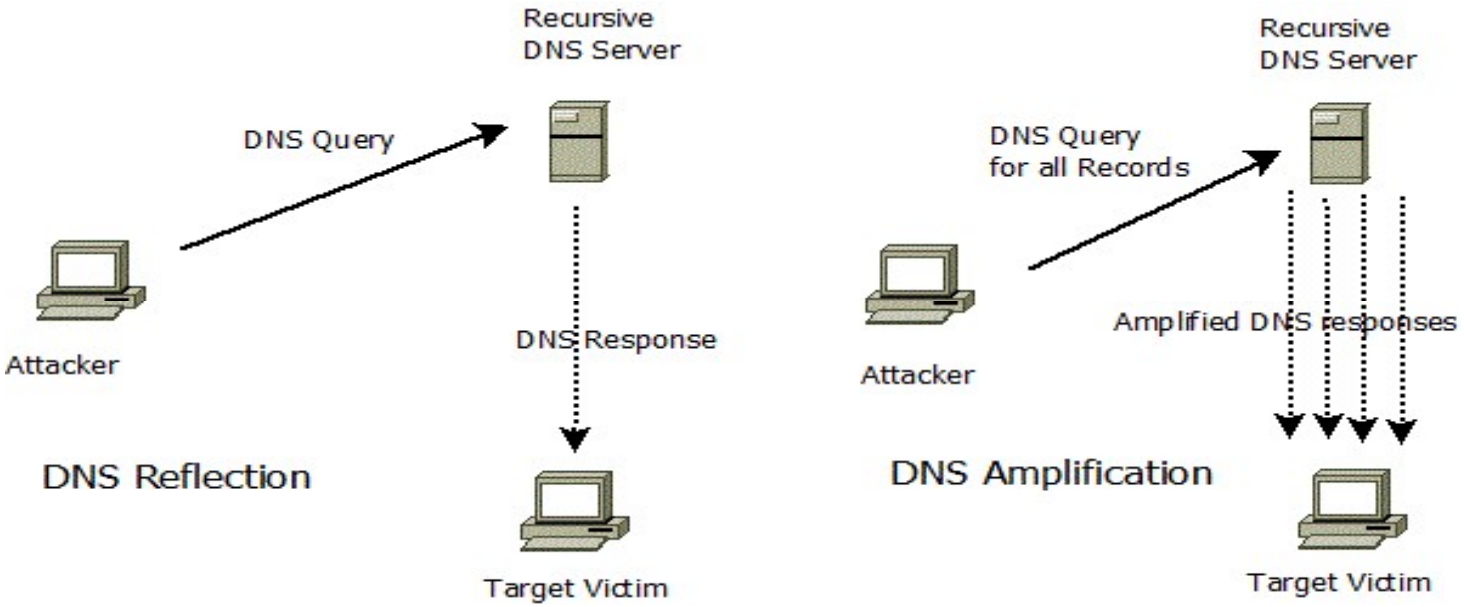
Attacks on DNS Infrastructure



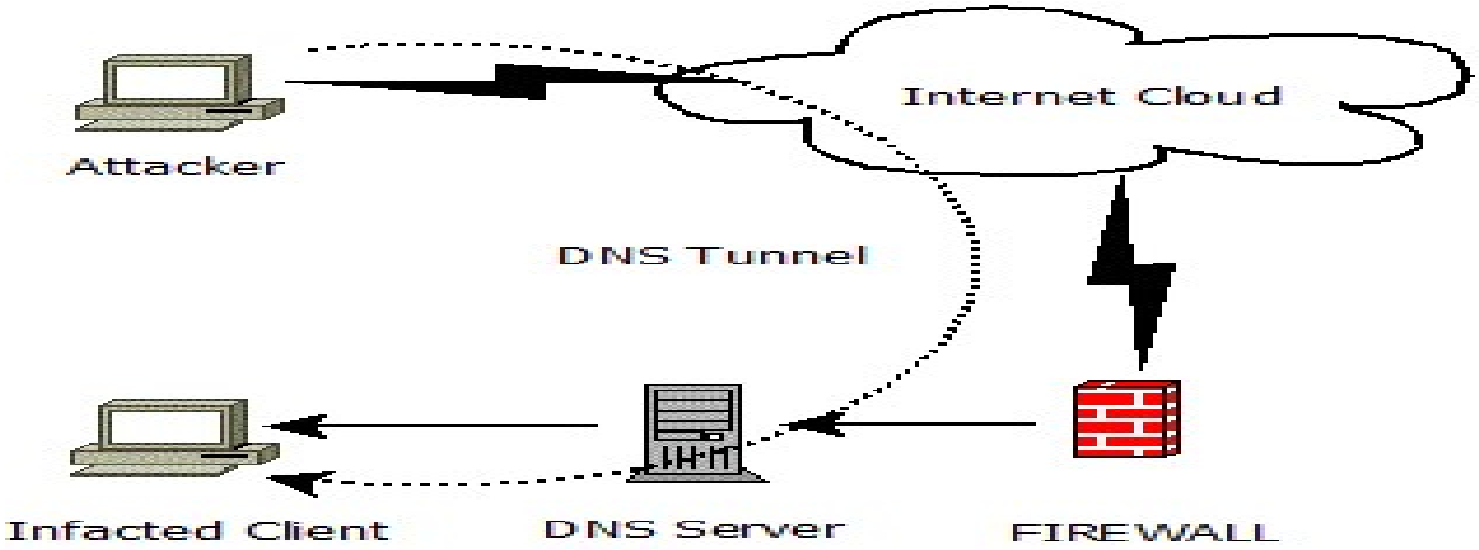
Attacks Exploiting DNS Infrastructure

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

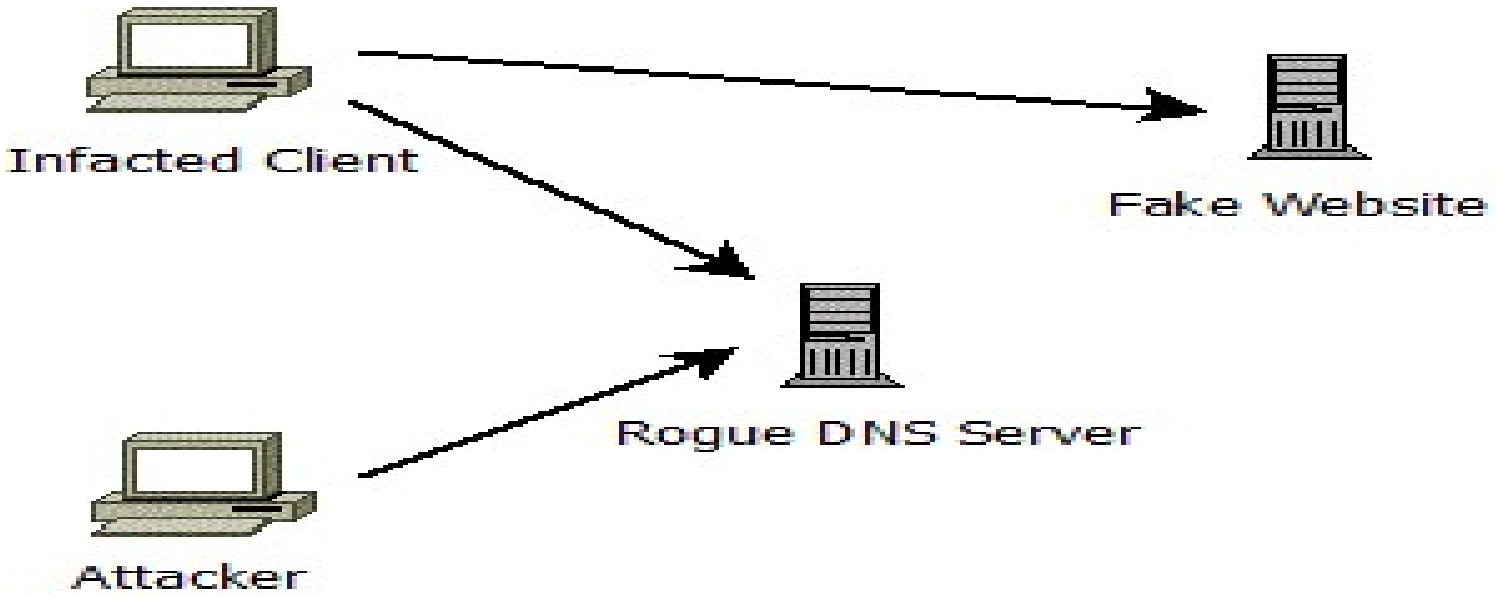
DNS Reflection and Amplification



DNS Tunnelling



DNS Hijacking



DNS Attacks Demonstration

- Reflection/Amplification
  - Dnsdrdos
  - Ethanwilloner DNS amplification Attack
  - Offensive python saddam amplification tool
- Demo of dnsdrdos tool

DNS Attacks Demonstration

- DNS Tunneling
  - Iodine
  - DNScat2
  - DNS2Tcp
- Demo of DNScat2

DNS Attacks Demonstration

- DNS cache poisoning
  - Msfconsole
  - Bind 9.3.* or earlier
  - Kali Linux
- Demo

Thank You

- Queries?
  - Sanjayadiwal@cdac.in