CSE 406

Computer Security

Project Design Report

DoS attack to the DNS server (using spoofed IP address)

Name : Abdur Rahman Fahad
Std ID : 1605069
Group : 02
Lab Group : B1

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology

Definition of the attack

DoS attack (Denial-of-Service attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Here we will attack the DNS (Domain Name Server) using spoofed IP address. We will perform the attack by sending lots of meaningless DNS query to the DNS server.

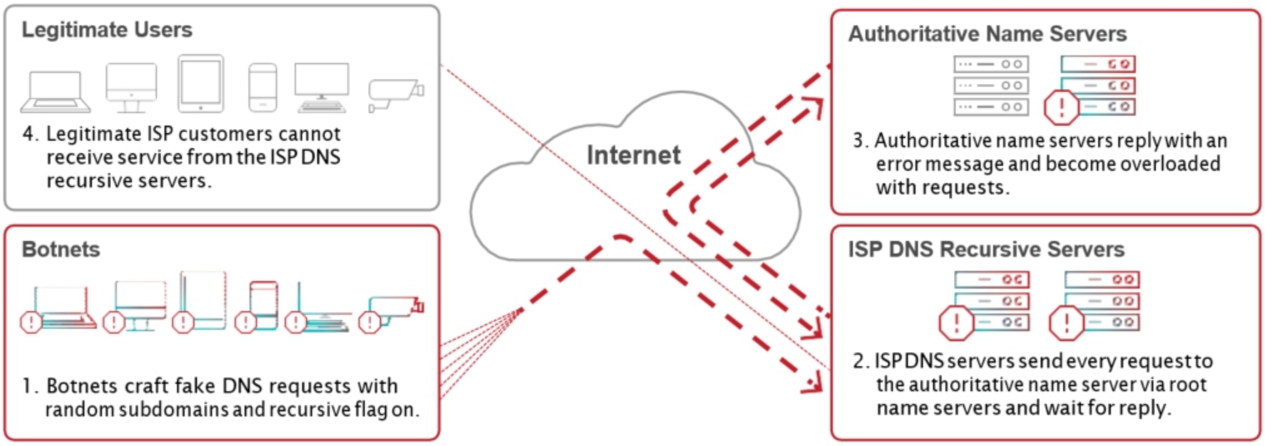

Legitimate Users
4. Legitimate ISP customers cannot receive service from the ISP DNS recursive servers.
Botnets
1. Botnets craft fake DNS requests with random subdomains and recursive flag on.
Internet
Authoritative Name Servers
3. Authoritative name servers reply with an error message and become overloaded with requests.
ISP DNS Recursive Servers
2. ISP DNS servers send every request to the authoritative name server via root name servers and wait for reply.

Figure : Topology Diagram of the attack

Timing Diagrams

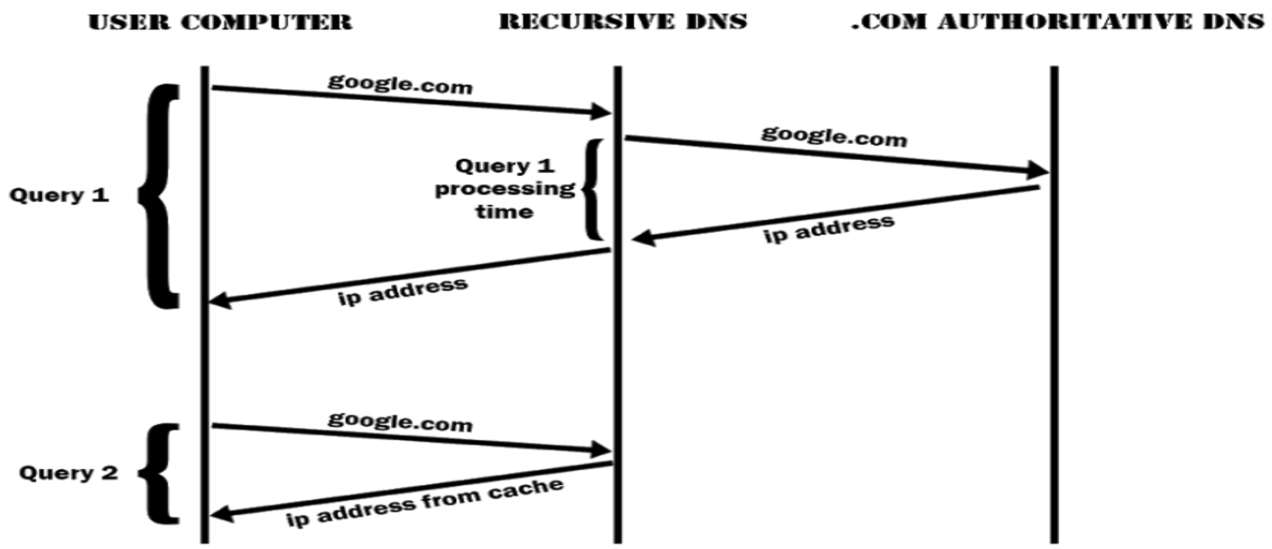


Figure : Timing Diagram of a DNS Query

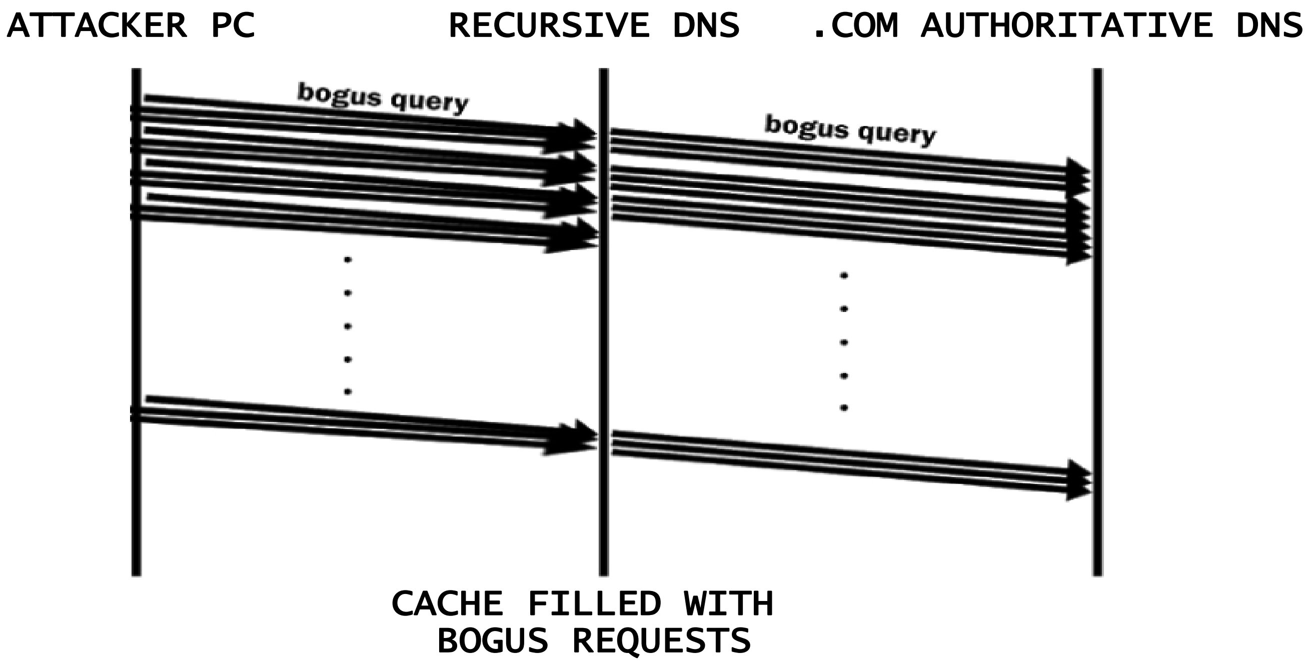


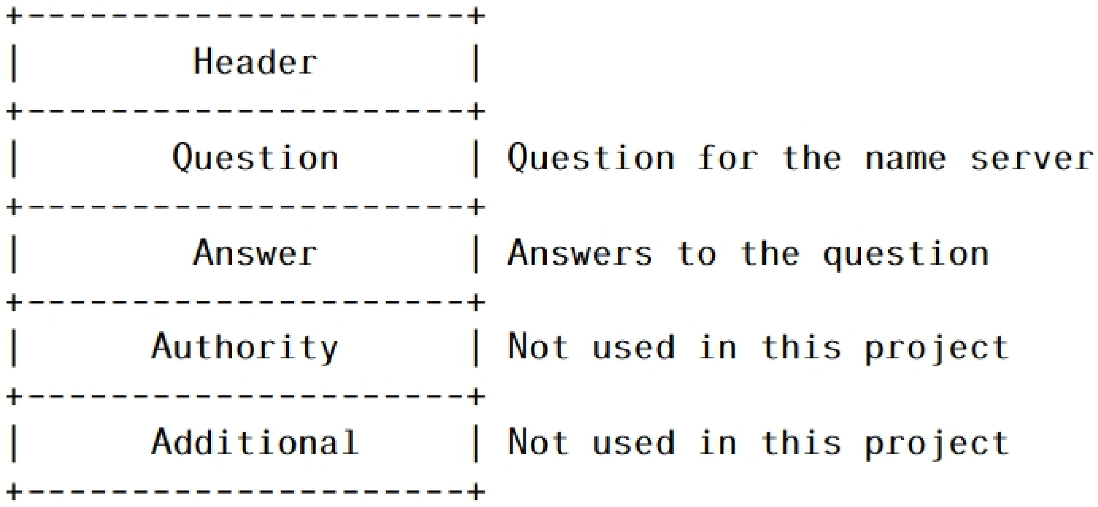
Figure : Timing Diagram of a DOS Attack on DNS Server

Attack Strategy

- We'll be using a local DNS server, which we'll attack. We'll configure a custom DNS server with a tool called Bind9.
- We'll flood the server with bogus DNS queries with unlimited UDP requests through our script.
- We'll change our IP continuously with the help of our script.
- We'll make our own packets for the DNS queries in which we'll set IP header as we wish, thus attack with spoofed IP will be possible.
- Thus the DNS server will run out of resources and any legit user will not be able to use DNS server.

Packet details and IP header modification

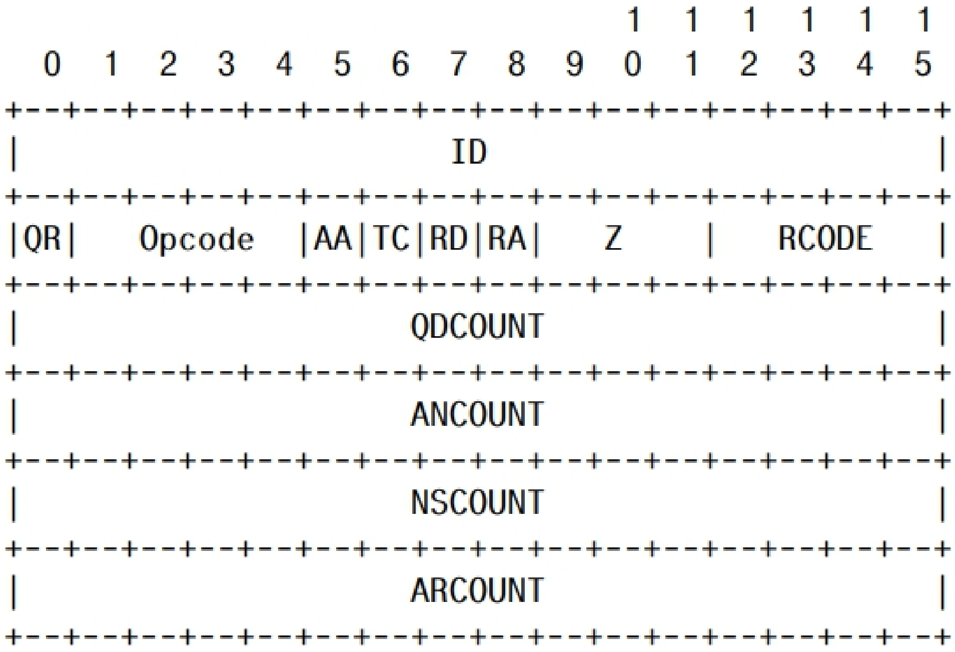
A standard DNS query packet looks like this,



```
+---------------------+
|        Header       |
+---------------------+
|       Question      | Question for the name server
+---------------------+
|        Answer       | Answers to the question
+---------------------+
|      Authority      | Not used in this project
+---------------------+
|      Additional     | Not used in this project
+---------------------+
```

Figure : DNS Packet Structure

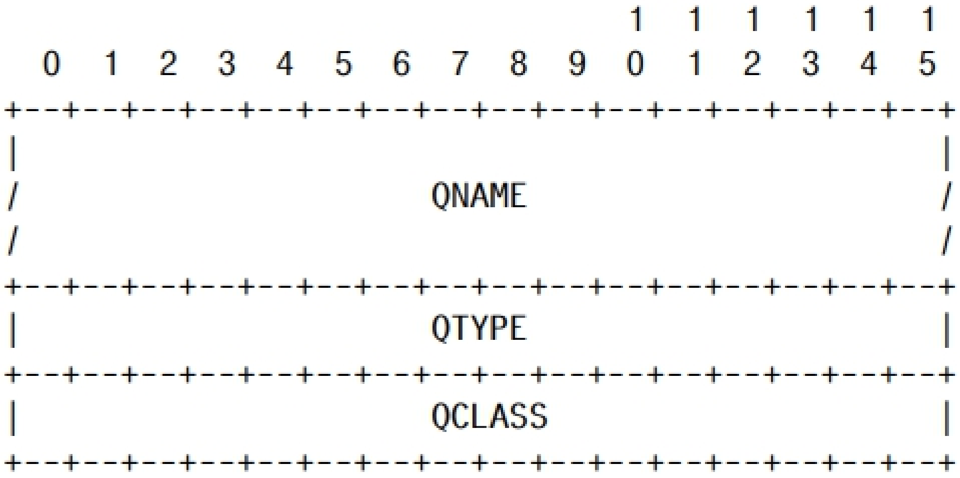
DNS packets have a header that is shown below.



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Figure : DNS Packet Header Structure

A DNS question has the format



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                               |
/                     QNAME                     /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                     QTYPE                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                     QCLASS                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Figure : DNS Question Structure

IP Header has the following format

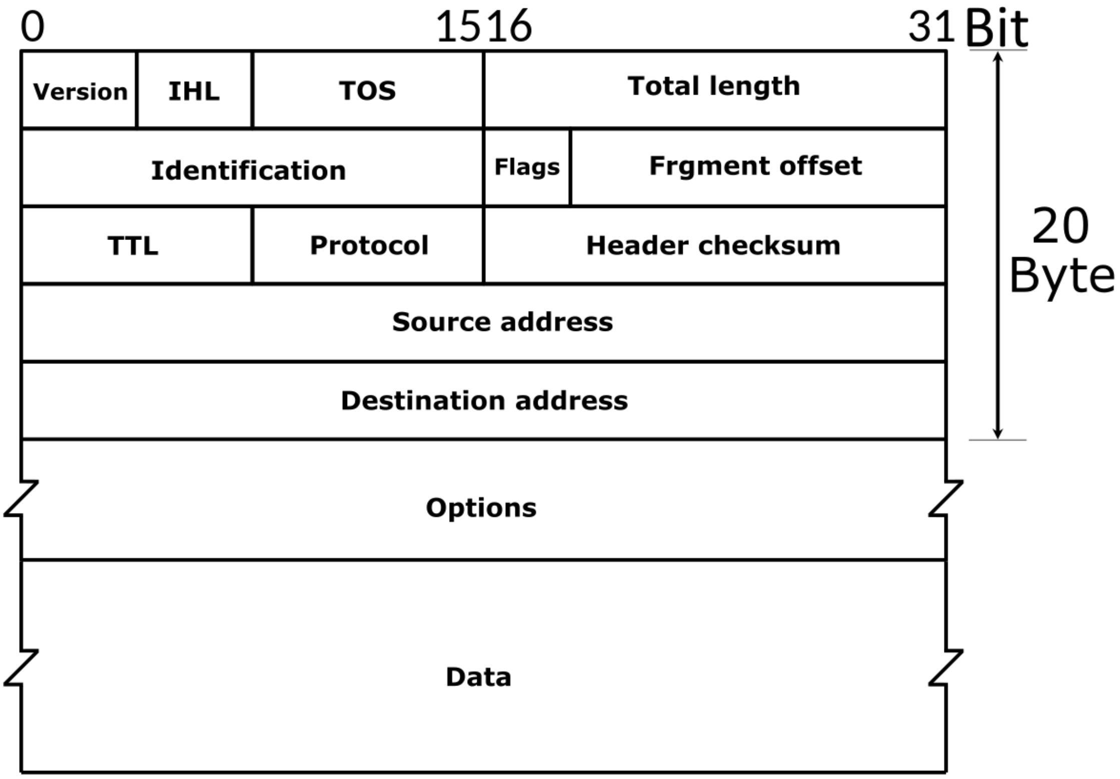


Figure : IP Header Structure

We’ll modify the Source Address in the IP header to implement spoofed IP address.

Justification

We will send bogus queries to DNS Server with a spoofed IP address in the source IP address field of IP Header. It’ll fail to find a valid entry in cache and so, the DNS server will send the query to authoritative DNS Servers and wait for the result, which will also eventually be failed.

By doing this with many infinite loop and many more requests than usual, eventually the cache of DNS server will be filled with bad requests. This way, it is possible to flood the targeted DNS and the server will deny any further service from any legit user and our attack will be successful.