CSE 410
Computer Security Sessional

DoS Attack to DNS Server

Soumit Kanti Saha
1505047

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
(BUET)
Dhaka 1000

DoS Attack to DNS Server(using IP Spoofing) :

DoS Attack to DNS Server in which the attacker targets one or more Domain Name System (DNS) servers belonging to a given zone, attempting to hamper resolution of resource records of that zone and its sub-zones.

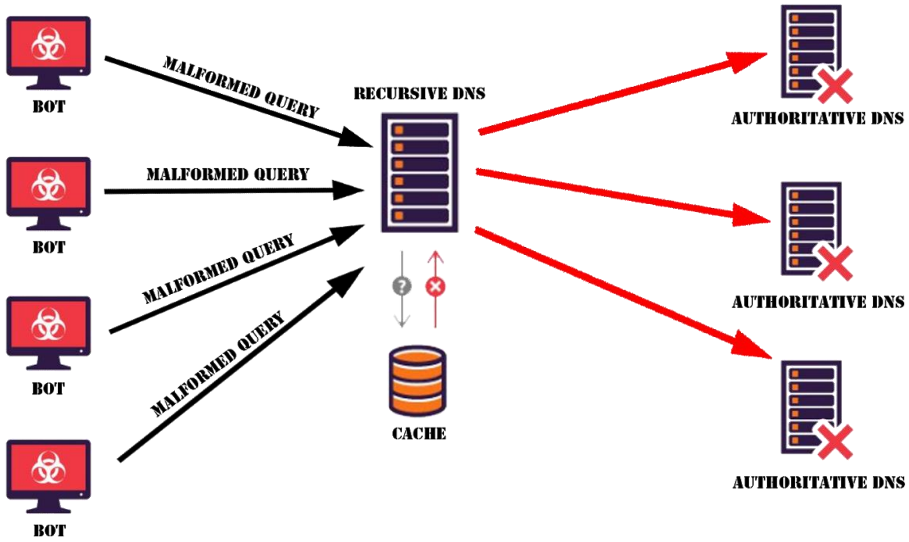


FIG : DDoS ATTACK ON DNS SERVER

I. Attacking Strategy:

1. We will make a symmetrical DDoS attack on a DNS Server. Our main target will be exhaust the server's memory or CPU with a flood of UDP request, generated by scripts running on several compromised botnet machines.

2. DNS servers rely on the UDP protocol for name resolution. With UDP-based queries (unlike TCP queries), a full circuit is never established, and thus spoofing is more easily accomplished.We will open a half completed circuit and change ip continuously.

3. Our programme will send malformed packets from spoofed ip address. As an application layer attack our programme doesn't need any effective response, we can send packets that are neither accurate nor even correctly formatted. We'll also randomize packet data which will help us to avoid common DDoS protection mechanism.

II. Timing Diagram:

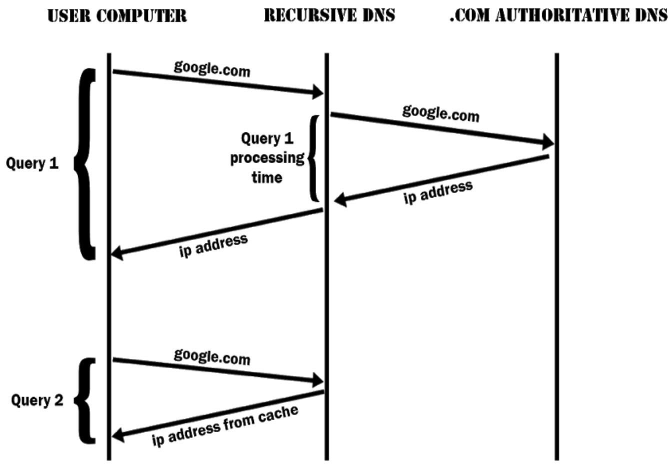


FIG: TIMING DIAGRAM OF A NORMAL DNS QUERY

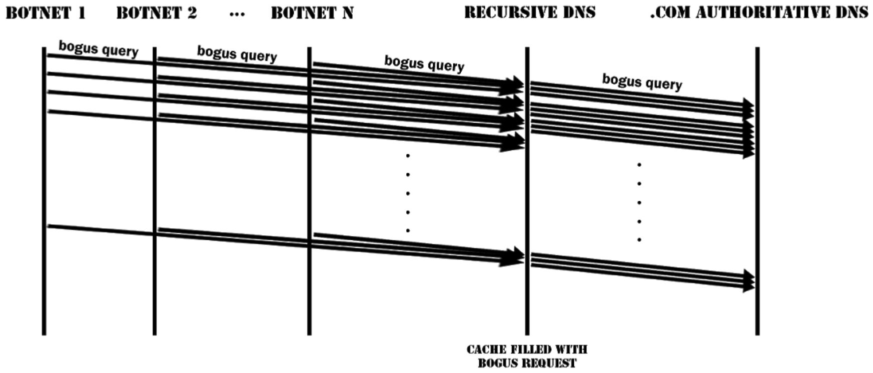
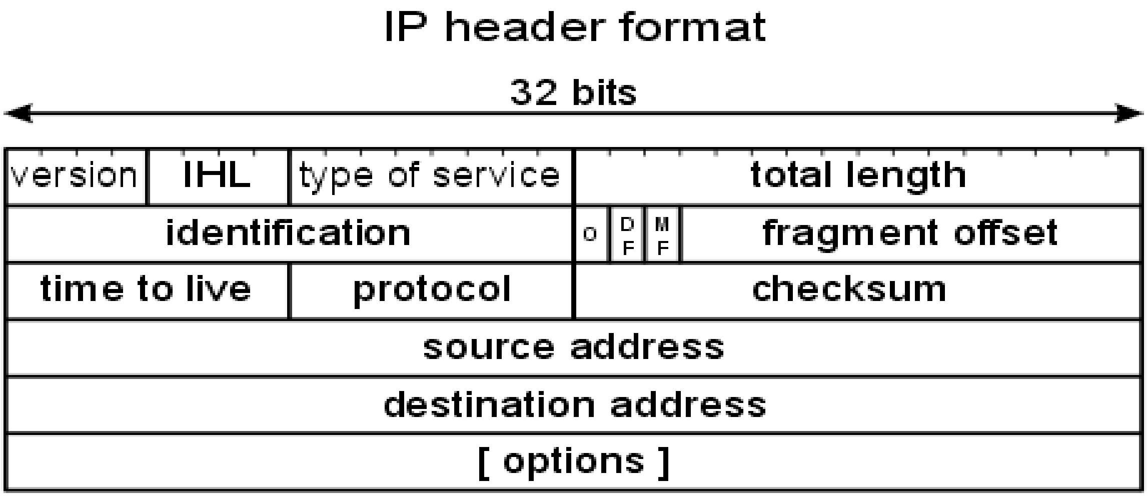


FIG: TIMING DIAGRAM OF DDoS ATTACK

III. IP Header Modification:



In the source address field, we will use spoofed IP address. This will be good enough to go.

IV. Justification:

1. We will send ill-formed queries to DNS Server with a spoofed IP address in the source IP address field of IP Header.
2. 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.
3. By doing this with many BOT computers and many more requests than usual, eventually the cache of DNS server will be filled with bad requests and with enough BOT computers, it is possible to flood the targeted DNS.

V. Virtual DNS Server: For testing we will use Bind9 to configure a DNS server on Linux host.

VI. Query type to DNS Server : We will only send question (type_A) query to DNS Server with query name (i.e. www.randombogusquery.com) which will not be an actual query name.