National Conference on Trends & Technologies in Multi-Disciplinary Research
Organized by A2Z Edu-LearningHub and
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 3 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

# An Approach on DNS Amplification Attacks

**Spartacus P.P[1], Jerin Joy[1], Nimitha Mohan[2]**
[1]Student, Department of BCA, SNGIST Arts & Science College, North Paravur, Kerala, India
[2]Assistant professor, Department of CS, SNGIST Arts & Science College, North Paravur, Kerala, India

## ABSTRACT

Attackers use DNS as a weapon against unsuspecting victims to bring down their websites. In the past and now in the present Domain Name Servers are under the threat of DOS attacks. This kind of attack takes benefit of the fact that DNS response message may be substantially bigger than DNS query message. The attackers vastly exploit open recursive DNS servers mainly for performing bandwidth consumption DDos attack. In this paper our analysis is based on DNS amplification attacks and ways of DNS attacks protection.

**Keywords :** DNS, DDOS, amplification, DNSSEC

## I. INTRODUCTION

Internet is growing day by day with new development and users. Also attackers still there in order to achieve an unauthorized access or to cause a DOS in the provided service.

DOS attacks can be classified into 2; First one is ping of death, adversely featly craft packets try to utilize the vulnerabilities in the implemented software (service or protocol) at the target side. In the second one; the attackers attempt to overwhelm critical system's resources. i.e. memory, cpu, network bandwidth by creating numerous of well-formed but bogus request. This type of attack is also well known as flooding.

As we know, computers can't understand our language and they go by numbers which means they use numbers to operate, communicate and store data eg: I p address,PID,0's and 1's.

DNS is an acronym for Domain Name System which contains number like physical address instead of human readable domain name like example.com. DNS resolves domain name to I p addresses. When a user enters a web address into a web browser, DNS will resolve the name to I p addresses. So this is how DNS server works. When we move through the timeline of networking, one of the most recent attack are reported in October 2002, 8 out of 10 root DNS servers were a massive DOS attacks and move attacks were triggered against these DNS in 2003 and 2004.Also in February 2004, name servers hosting top-level Domain [TLD] zones were the frequent victims of vast heavy traffic loads.

In this research paper, our centre of attention is DNS amplification attacks, types and prevention.

## II. DNS SECURITY ISSUES AND VULNERABILITIES

The Domain Name System is hierarchical, distributed database that maps human readable domain names to I p address, DNS help users to find resources on the network by converting human readable names like xyz.com to ip address that computer can connect to. DNS is like an index of book which by converting the domain names to unique ip address. For example www.abcd.com translates to the addresses 20.52.88.12. DNS is one of the most crucial parts of a computer networking and scuring it is most important task. If we make compromised, an attacker can easily prevent normal operations going in the network, can route computer to whatever spoofed ip address they like and steal information.

**The Domain Name System are still under cyber-attacks. There are many relevant threats:**
DDos attacks on name servers: attacker targets one or more DNS servers belonging to a given zone, attempting to obstruct resolution of resource records of that zone and its sub-zones. DDOS attacks are from multiple sources, DDoS attacks achieve effectiveness by using multiple computer systems as sources of attack traffic. Usually, attackers deploy bots to attacks the target with traffic. If the attacks are from a single source or computer is known as a Denial of Service (DoS) attack and is mostly has minimal effect.

**DNS amplification attacks:** DNS amplification is an asymmetrical DDoS attack in which the attacker can send small query with spoofed target IP, making the spoofed target the recipient of much larger DNS responses. With these attacks, the attacker's goal is to overload the network by continuously exhausting bandwidth capacity.

**DNS spoofing:** it is also known as cache poisoning which is attacker stores corrupted or incorrect data in dns resolver's cache. These lead users to incorrect websites instead of actual website.
Cache poisoning attacks typically occurs in a way that the attackers impersonate a DNS name server
They send request to a DNS resolver
They forge a reply to the DNS resolver before the actual DNS name server can answer.

**DNS has three major vulnerabilities in which attackers often exploit to abuse DNS:**
All the server names and IP addresses for their domains are stored in Internal DNS servers and will share them with anyone that asks.
So the DNS plenty of information for attackers when they're trying to do internal reconnaissance.
DNS caches aren't "authoritative, and they can be mishandled or corrupted.
If your DNS server is "poisoned" with bad records, this leads computer to location instead actual one.
DNS relays query information from internal workstations to outside servers, and attackers have learned the way to use this behavior to form "covert channels" to exfiltrate data.
Internally, one of the largest threats to DNS infrastructure is the DNS server itself. DNS server software is complex, with millions of lines of
code, and that much code is going to avoidably result in vulnerabilities that an attacker can gain access to a network.

## III. DNS AMPLIFICATION ATTACKS

### 1. DNS Spoofing

A DNS spoofing attack is one in which a victim, or victims, is misleaded along DNS to a host that is not the desired destination. Cache poisoning is one type of DNS spoofing attack, but there are many other types of DNS spoofing attacks that do not affect cache poisoning at all.Trojan known as Win32.QHOST is one example for DNS spoofing.

A fle called hosts is built into all version of microsoft windows operating system. The file sits in the directory C:\%windir%\system32\drivers\etc
\hosts and is used to map IP addresses to system names or domains. The file is a reminder to days before DNS Existed, and it enables interaction among machines on a network regardless of whether or not DNS is configured. Typical hosts file looks
Like this:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# The following is a sample of HOSTS file developed by Microsoft TCP/IP for Windows.
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
```

A less common method of Domain Name Server spoofing is to use a specialized tool sitting on another host on the same network to ambush and react to DNS queries coming from the destination host. This method is a little more problematic
because it needs that the attacker already has the permission to the target network and is able to install a network sniffer on the network without being identified.
One of the tools that can be used for this type of attack is dnsspoof and it is one of the dnsniff penetration toolkit

## 2. Cache Poisoning

In a DNS cache poisoning attack intruder takes use of the weakness in the DNS protocol to load bad data into a recursive DNS server and that data usually involves transmitting a fake A record to the recursive server in order to divert traffic to infrastructure owned by the attacker. The simplest form of this attack is to send additional A records with a request to a malicious domain To understand how this attack would work, lets check the traditional DNS request from the victim perspective and the DNS recursive server perspective.
This is the user request:

```
[user@workstation B]# host dns-book.net dns-book.net
 has address 8.5.1.36
dns-book.net mail is handled by 10 p.nsm.ctmail.com.
```

The recursive DNS server checks for the A record, and it also checks for the MX record and stores it in its cache so if other clients of this recursive DNS server need that data it usually be available, at least until the Time to Live (TTL) expires.
In order to know how cache poisoning works, mainly we need to understand DNS at the packet level. A DNS packet includes three parts: Header, Question, and Answer .The header has a permenant size of 12 bytes while the Question and Answer sections differs in size. Because most DNS queries and returns are transferred over UDP, there is a packet size limit on the packet size of 512 bytes and also, because DNS and responses use UDP there is no handshake between the recursive and authentic name servers. Instead the DNS server depends on a combination of source port, original destination IP address, and a 16-bit transaction ID in order to certify an incoming return.Forging a DNS packet is commonly simple; by the way there are a number of tools that help spammers create a forged DNS packet and since the protocol is delivered using UDP forging an IP address is insignificant. A forceful tool for forging DNS, and other, packets is hping3. Using hping3 a spammer can create forged DNS packets that looks exact as they came form the random addresses:

```
[root@server B]# hping3 -2 -p 53 --rand-source 8.8.8.8
```

This command directs hping3 to forward DNS packets from randomly forged IP addresses to the name server 8.8.8.8.Another method of DNS cache poisoning is the local DNS cache poisoning attack. This attack does not cause the client's recursive DNS server; by the way it infects the DNS cache directly on the client's workstation. Many people doesnt know that, by default, Windows and Apple OS X workstations keep continuing a local DNS cache based on responses from the organized recursive server. The local cache boosts the method of visiting recurring queried domain names. Unfortunately, this is also insignificant attack vector to exploit.

### 3. DDOS using DNS

A DNS-based DDoS attack simply means sending more traffic to a target server in which server can't process. At that point, the services on the server become unavailable and legitimate users may not able to access them or can only access those services sometimes or infrequently.

There are a number of tools are used to launch this type of straightforward DDoS attack, probably one of the best known is Low Orbit Ion Cannon(LOIC), LOIC was originally developed in 2004.This tool was widely used by attackers because it is simple to use and both runs n windows and linux platforms. It is also versatile in which it can be used to create attacks against a various services running on a target host.

While the tool is easy to use, it is not covert. All of the packets launched from the tool are directly tied to the attacker. However, when used as part of a larger group, unlikely any of the attackers will be singled out for execution.

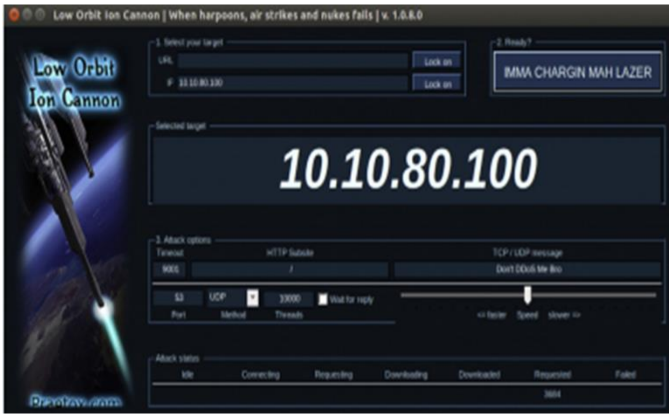
DNS amplification attacks are DNS DDoS attacks, a series of small DNS Queries used to generate larger DNS responses. By ip spoofing these responses are directed toward a target host. This type of attack may include up to three different victims. The first victim could be the host or attacker launching the query with target address and may be an unwitting member of a botnet, unaware that malware being used in a DDoS attack is installed on his/her computer. The second victim is the DNS server that is being queried by the victim hosts and the third victim is the target itself.

To understand how these attacks work, take a look at this dig request:

Where the dig is a command used in DNS servers for querying for information about host address and related information

```
dig@PDNS-PUBLIC-NS1.POWERDNS.COM
powerdns.com ANY 1 dnssec
```

The query is pretty simple; it asks the Power DNS name server to provide all known records for the domain powerdns.com. The query also asks for any DNSSEC information. At 17 bytes the query is a small one, as shown in this tcpdump output:



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

IP 10.10.80.100

Selected target

10.10.80.100

3. Attack options

Timeout 9001

HTTP Subsite /

TCP / UDP message Don't DDoS Me Bro

Port 53

Method UDP

Threads 10000

Requested 3664

```
0:41:56.231234 IP (tos 0x0, ttl 53, id 37793, offset 0, flags [ 1 ], proto:
UDP (17), length: 1500) 188.166.104.87.domain . 192.168.1.15.49890:
57446-| q: ANY? powerdns.com. 14/0/1 powerdns.com. Type46[|domain]
```

However, it returns a big response, the dig output shows that the resulting response switched to TCP and returned 2977 bytes.

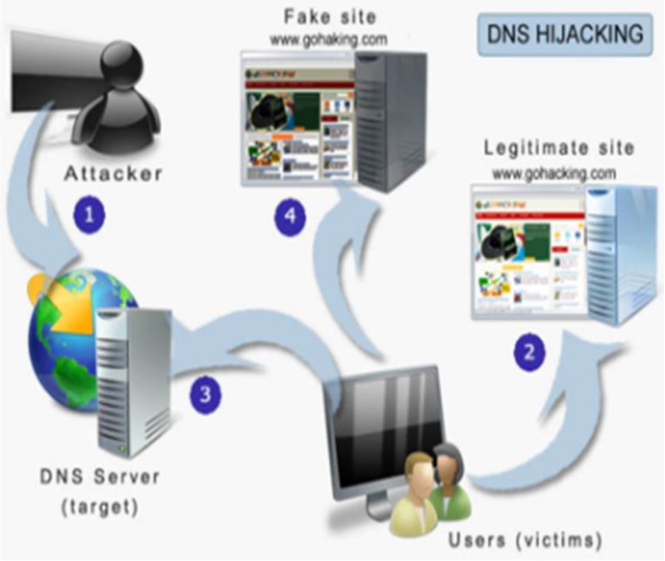
;; Query time: 82 msec
;; SERVER: 188.166.104.87#53(188.166.104.87)
;; WHEN: Mon Feb 1 00:41:56 2016
;; MSG SIZE rcvd: 2977 in other words, this response is 175 times larger than the query used. An attacker Can controls thousands of hosts within a botnet can easily send thousands of queries from the victim botnet members within a certain period of time to the

DNS server and direct the results of those queries to the target host, easily taking it off-line. Using a small query to produce a large amount data and redirect that large data into a victim Server.

## IV. DNS HIJACKING

Attackers get benefits of the DNS system to send victims to fake websites address, using a technique called DNS hijacking.

In DNS hijacking, attackers redirect their victims away from the popular websites that they want to visit, using DNS-related tricks to bring them to fraudulent sites. These fake websites are generally designed to look like the legitimate site, and aim to steal the victims login credentials or credit card details. Hackers then use this information to access their commit fraud or accounts and other crimes.



In another way, through DNS hijacking attacker send victims to websites that host malware. This could consist of ransom ware, spyware, adware, Trojans and a range of other malicious programs. Using these malware hackers can get and operate whatever he want to do in victim side, use its information to threat, access accounts and money. The attacker user's different types of techniques to redirect user from intended websites to malicious page.

- **Local hijacking** – in this type of DNS hijacking includes an attacker installing malware on a target victim's computer, then changing the local DNS settings to divert them to a malicious site instead of the intended webpage.
- **Router hijacking** – Attackers can take advantage having Routers firmware vulnerabilities or still using default passwords. So this security weaknesses,make the attackers to access and reconfigure the router's DNS settings. If they change the DNS settings for certain sites to those of a malicious site, any victim connecting through the router will be diverted to the malicious site when they try to access the websites that had been altered.
- **Compromised server** – Hackers can compromise DNS servers and update their configurations so that the IP addresses of targeted websites actually point to sites under the control of the attackers. When a victim's machine sends a DNS request to one of the targeted websites on the compromised server will be redirected to the malicious website, where they might encounter malware, phishing or pharming.
- **Man-in-the-middle DNS hijacking** – In a man-in-the-middle attack, cybercriminals put themselves into a communication channel and either listen or alter the messages.by intercepting the messages sent between a DNS server and a user. The attacker alters the DNS server's response to the IP address of their malicious website, redirecting the user to the malicious site.

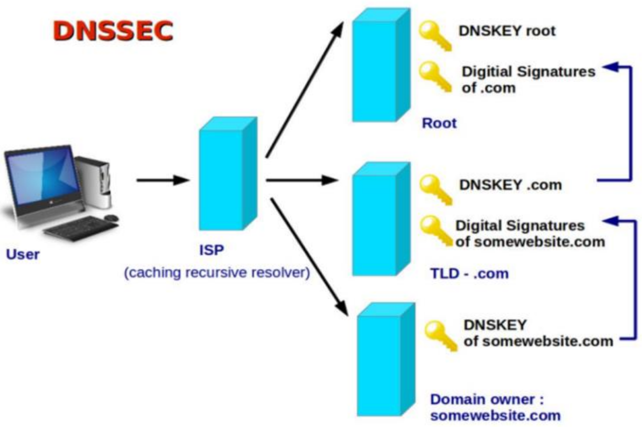
## V. DNS SECURITY BEST PRACTICES

- Enable DNS logging-Most efficient to monitor dns activity is dns logging. Using logs ,it let you know if someone mess with your DNS server. Unlike client activity, debug logs shows when there are issues with DNS queries or updates. DNS logs also results the traces of cache poisoning. In case of cache poisoning, an attacker change the data stored in the DNS cache and send to clients. For example, an IP address of www.facebook.com might be changed to an IP address of a malicious site. When a client sends a query to DNS for facebook.com, the server redirect with the wrong IP. Users then visit websites they intended to visit instead of actual and become a target of hackers. To achieve better performance, some system admins decide to disable DNS debug logging. Monitoring network activity can help you identify some attacks, such as DDoS, but not cache poisoning. Therefore, enabling DNS debug logs is good in informing attacks.

- Lock DNS Cache-DNS finds the information corresponds to the query from client and stores it in the cache for future use. Through this process server can respond faster to the same queries and fetch information from cache .but Attackers utilize this feature by altering the stored information. By enabling DNS debug logs is locking DNS cache. If cache locking is deactivated, then information can be overwritten before the TTL expires. This leaves room for cache poisoning attacks.
- Filter DNS Requests to Block Malicious Domains-DNS filtering is an effective way to block users from accessing a domain, if domain is known to be malicious. DNS server stops client when client query for a blocked website. DNS filtering greatly reduces the possibilities of viruses and malware reaching your network.
- Validate DNS Data Integrity with DNSSEC [Domain Name System Security Extensions] DNSSEC secure clients receive valid responses to their queries. Data integrity is achieved by DNSSEC .When an end-user sends a query; a DNS server provides a digital signature with the response. Hence, clients receive valid data for the request they sent. Since DNSSEC provides data integrity and origin authority, DNS spoofing attacks and cache poisoning are successfully prevented.
- Configure Access Control Lists-It covers DNS servers against unauthorized access and spoofing attacks.

## VI. PREVENTION TO DNS AMPLIFICATION

- DNSSEC - DNSSEC establish a trust chain between the user and authoritative server.when a user sends a query,the DNS server provides a digital signature along with the response.Based on a key exchange inside specific signed resource record.


DNSSEC
DNSKEY root
Digitial Signatures of .com
Root
DNSKEY .com
Digital Signatures of somewebsite.com
TLD - .com
DNSKEY of somewebsite.com
Domain owner : somewebsite.com
User
ISP
(caching recursive resolver)

- Maintaining Your System Up to Date .Updates latest version of all software and programs aiming its security.
- Prevent resolver from cache poisoning, so it is kept restricted from external user.
- The cache in DNS should clear on both local as well as extensive area networks.
- Installing a reliable and powerful firewall is the best way in preventing DDoS attacks.

## VII. CONCLUSION

We have presented our analysis about DNS attacks.And discussed types of DNS amplification attacks. Also the weakness in the DNS systems and ways to its protection.

DNS is the backbone of internet. Much of the DNS infrastructure has flaws, unprotected and under threat of attackers.so it requires more updations to make it secured. DNSSEC was one of the best security practices for DNS server's .In future still has chances for more aggressor attacks can be done. From now we can initiate to build programs and techniques can be implemented at DNS servers and requires new research in building a powerful DNS infrastructure.

## VIII. REFERENCES

[1]. Cert Advisory CA-1996-26, "Denial of Service Attack via ping", http://www.cert.org/advisories/CA-1996- 26.html, December 1997.

[2]. Michael Dooley ,Timothy Rooney " DNS Security management" Published by John Wiley & Sons, Inc., Hoboken, New Jersey

[3]. Adam Ali.Zare Hudaib, Esra's Ali Zare Hudaib "DNS advanced attacks and analysis" International Journal of Computer Science And Security, Volume(8): Issue(2) :2014

[4]. Thijs Rozekrans"Defending against DNS reflection amplification attacks" February 14, 2013

[5]. Geogios Kambourakis,Dimitris Geneiatakis "Detcting DNS Amplification Attacks" October 2007