ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Deficiency and Secure the Attack Superficies to Your Organization Localization Main DNS SERVER

Yashpal*, Prof. (Dr.) Rajesh Bhagat, Diwaker
*M.Tech Scholar in CSE from JB Institute of Technology Affiliated to Uttarakhand Technical University, India
M.Tech (CS), M.Phil (CS) and PhD (CS), PhD (Mgnt), India
NITTTR Chandigarh Technical Institutions, India

Abstract

The Domain Name System (DNS) numeric instead of IP address and other Organizations for network of communication of difficult to remember to use Fully Qualified Domain Name (FQDNs) and using identification of hosts on the internet one way to provides a system that is. The Domain Name System (DNS) without you all its network Client server and remember the IP address will be forced to. In the number of attacks on the internet it was available for the common people When is has increased. That has been attacked constantly services from a Domain Name System (DNS). A most important part of outside and inside to queries etc. The Domain Name System (DNS) service employment attacks in major types one attacker fake DNS query sends reactions instead of and valid IP its And, therefore, cache response to user on the site was malicious server will be nominated again Domain Name System (DNS) cache where vicious include . Against the attacks of such for the defense of, a number of research methods have been with and success separate, is implemented. Many steps in this letter to influence them Domain Name System (DNS) service and Information attacks is taken to achieve. Analysis of various attacks possible that and described. Attacks to find out the features of attack done by analysis and Address Methods of imposing is derived. That will be presented in this letter target Domain Name System (DNS) server connected with this kind of attacks on to pick center. The simulated local demand for this kind of attacks out and therefore this kind of attacks in the future to prevent on to search for new measures necessary to identify important steps will be helpful in.

Keywords: -Introduction and Introductory and connected work, Classification and overview of attack, Deficiency &secure to localization DNS Server

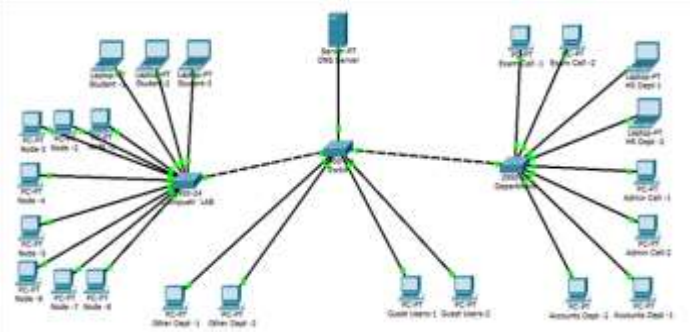
Introduction

The Internet for the common people has been available after on internet services number of attacks is growing. Using different methods of attack also that services from a Domain Name System (DNS) of Service. An important part of Internet IP address resolution and In contrast to host name is used for Domain Name System (DNS) and Without DNS this mechanism may not easily. The new services almost daily attacks Domain Name System (DNS) architecture because of existing weaknesses to appear. To find out the attacks the characteristics attack and is done by methods of detection is derived. The will be presented Domain Name System (DNS) server target connected with this kind of the attacks to pick cantered on. This Attacks of the simulated take out for such in future and therefore Attacks on new measures to prevent necessary to search for important steps helpful in identification of will be.A DNS Client server network attackers or use for traffic they have a DNS client or server DNS query and sent a DNS Wait for reaction is that it seems that in to may be able. This matter is true for they have fixed, the attackers one or more packet fake Domain Name System (DNS) reaction back to send and authentic requestor reaction to green Can efforts for. The one attacker to send DNS customers and remote DNS questions on the server that DNS can attack. They are attackers from time-to-live (TTL) fake response that has assigned to control because of the attack of successful Later, this is also now day, week, or continues for can [7].

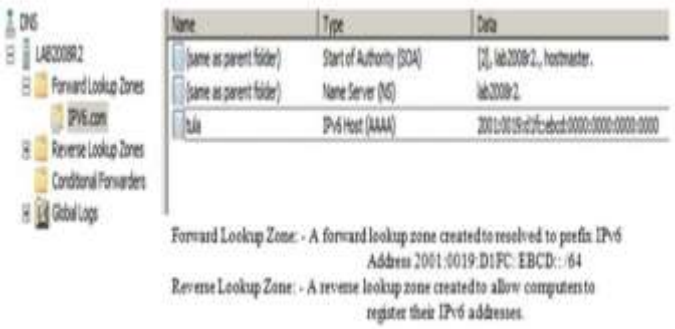
Introductory and connected work:-TheDomain Name System (DNS) Name a tree or categorized uses structure, Internet on IP address domain and hierarchical name. At the top of the tree top-level

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

domain (TLDs) Lower level, the domain name and number of And dot of each stage is by root chase (.). The Domain Name System, or DNS, The map between hostname and IP addresses, and routing for providing electronic mail information TCP / IP It is used by applications that are a distributed database. We all the information on the internet site knows no distributed because Use the period. The each site (for example a company for university withindepartment, complex, company, or department), Information His own maintains the database and Internet (customers) throughout the other systems that can query a server Program runs. DNS client with one another and the Server Dialog allows toprotocol that provides [8].



i. **Domain Name System (DNS) Queries :-**To customers to seek information from those people a DNS use the server .The request from the customers come directly, an application or customers are going . The customer (such as customer request that a special resource record, Usually on Internet which is domain name, As a class for a fully qualified domain name (FQDN), Thus, a query for which DNS server sends a query message) class. A customer used in a program to a name is, to solve this name from the server DNS asks. The Customer sent each query for replying to the messaging server three specific can request the information. It is a specific DNS domain name, one Specify type and DNS domain namequery for a specific Class [3].



ii. **Domain Name System (DNS) Message and Notification format: -** A character and they both. Each message header and in four sections constitutes: question, authority, right, and additional. 'Flag header sector 'these four sections of But all material structure of DNS messages are one control Clause areas header includes: Identification of questions , flag, Number, number of replies, Number of right resource record (RRs), The number of and additional RRs. The query area which identifies identity with 16 bit. The DNS Client Sector with a North using a query can email, Flag sector four bits together. A query message (0) or a reply (1) If first indication. Second For a small server DNS official if (only in a message) when asked is set hostname. The third bit is set to (1) a customer wants to send recurring query[6].

Expedient Types	Characterization	Usage / Proceeding
A	An address record	Maps FQDN into an IP address (only for IPv4 IP address)
AAA	An address record	Maps FQDN into an IP address (only for IPv6 IP address)
NS	A Name Server record	Denotes a name server for a zone
PTR	A Pointer record	Maps an IP address into FQDN (fully qualified domain name)
SOA	A Start of Authority record	A start of authority (SOA) record is information stored in a domain name system (DNS) and Forward Lookup Zone or Reverse Lookup Zone administrative contact, the serial number of the zone, refresh interval, retry interval, etc.
CNAME	A canonical name record	Defines an alias name and maps it to the absolute (canonical) name
MX	A Mail Exchanger record	Used to redirect email for a given domain or host to another host

Classification and overview of attack

The attackers in these years in the form of circumventing last type of attacks fixed for defense against invented for circumventing demonstration attacks new ways to found. The DNS server

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

connected with two attacks large groups can be classified [3].

- The attacks destinationing to DNS Servers
- The attacks using DNS Servers, to destination some other side System

The some other system DNS rebinding attack for targeted DNS Server uses, While DNS server DNS Cache poisoning attack target. The one attacker a Domain or false solution for hosts DNS entries allowed on for in the absence of any verifies the signature makes it possible. The cache contaminates recurring enabled query or an end with hosts a DNS Can is on the server.The one of the hosts of the attack asks for the solution address that the time started on. The poison cache, this question would be accepted in their reply, that is being asked because DNS faster than query server response to will try to. The attacker work this address for resolution of which is DNS official DNS Server there is a need to server address and this DNS server on the address of its the source is a need to address fraud . An Approach answer in time Server is not an official DNS Distributed Denial of Service (DDoS) that the attacks on official DNS server slow performance to ensure that it to. The against this a security in DNS packet queries Equipment Interface Development (EID) because this kind of attack is possible. The before this in the time of QID after every query will be incremented by one, But it soon this is not provide security any realized that .The random number used nowadays applicable proxy generation all be DNS server Pseudo Random Number Generation (PRNG) query id QID for the region [1]. There are two types' attacks in you localization main DNS Server:-

A. Protocol Attacks

i. **SYN Flood: -** The configure data packet pate "per minutes" and the burst rate "per seconds" for source and destination. The SYN Flood is the attack in the large numbers of connections nods are sent so that the backlog queue overflows. The connections is created the victim hostreceives a connection request and allocates for it some memory resources. A SYN flood attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more [2].

ii. **User Datagram Protocol (UDP) Flood: -** The configure data packet pate "per minutes" and the burst rate "per seconds" for source and destination. The User Datagram Protocol (UDP) Flood links two systems. It hooks up one system's UDP character-generating service, with another system's UDP echo service. Once the link is made, the two systems are tied up exchanging a flood of meaningless data.

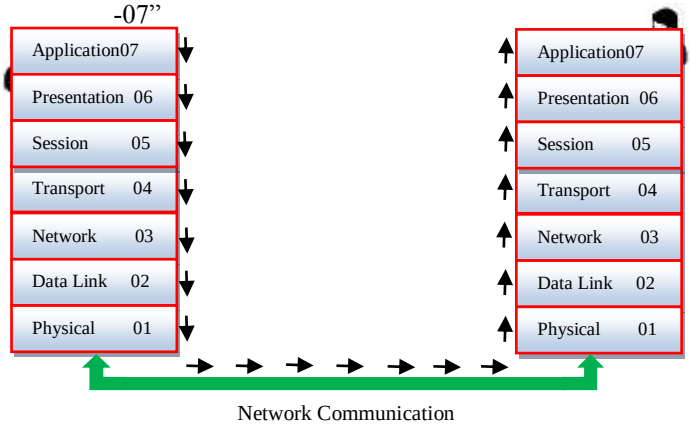
iii. **The Transmit Control Protocol (TCP) Flood: -** The configure data packet pate "per minutes" and the burst rate "per seconds" for source and destination. The Transmit Control Protocol (TCP) attack sends huge amount of TCP packet so that the host/victim computer cannot handle.

iv. **ICMPv4/ICMPv6 Flood: -** The configure data packet pate "per minutes" and the burst rate "per seconds" for source and destination. The ICMPv4/ICMPv6 attack sends huge amount of packet/traffic so that the protocol implementation of the host/victim computer cannot handle [2].

B. Application Attacks: - The application layer attacks are here to stay and we should expect more of them. The first of these attacks being successful, it's up to us on the same subject with more changes will see more of them became a certain condition. The more and more organizations in the transport and application layers in the network layer, but it's not above them shower strikes, are reported. The best for secure coding course will solve this, you might think. But to rule the rising attacks are so prevalent that even today there are attacks SQL, XXS, Spam, Data leaks, Encryption and injection etc. Thegrowing more data centers and clouds are feeding on the world's resources that are more and more subtle attacks; Data about injecting malicious code into a nasty fingering are not spread around like [5].

i. HTTP attacks on web server "Layer -07"

ii. The web application attacks on CPU "Layer -07"

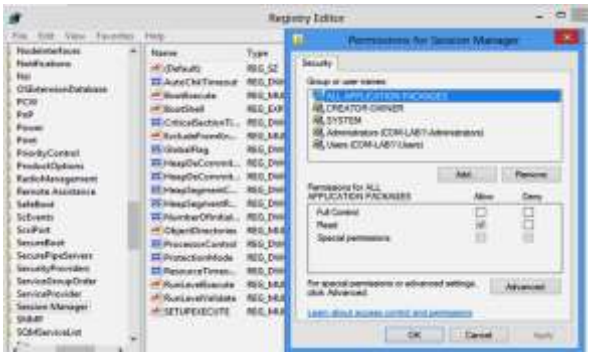


ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

The DNS Server day by day can face is a distributed denial of service (DDoS) attack. The unfortunately, this kind of attack in recent years has become very popular, and very low to stop it fully can be. When you are composing attackers target the server will use many strategies. When you send recently, in the use of propagation DNS we begin resurgence is DDoS attacks. However, only a few steps use your DNS server is being the risk of this kind of attacks and for being part of both in the resolution unless DNS attacking one such attack problems. One of the consequences of there were in the form of from becoming unresponsive DNS server for the defensive of their at least can be taken for TCP and firewall for UDP PORT 53 have been allowed through.The port no. 53 default you are DNS Server machine [4].

i. **DNS firewalls to access and Authorization control: -** Your Firewall Prompts DNS can connect to server Access On To achieve control can be used. Only Internal customer is used for questions that DNS Server, for those DNS server connection to external hosts block Click Firewall Prompts configuration to. Caching-only DNS forwardersused as to the server, Only Caching - who only to use the forwardersDNS from the server Questions for allowing your Firewall Prompts configuration. As a special Important external DNS firewall policy settings from the server to connect to use the internal DNS Protocol Users to the block.
   - **Authorization =The Authorization**process of granting approval or permission on resources.
   - **Authentication=** TheAuthentication is the process or verifies the identity of a users.

ii. **The Clients / Users privileged polices modify controls on DNS registry and script Entries :-** There is a need for access to those accounts that only those Registry settings To read or change is allowed for Microsoft, Windows and Red Hat based server DNS relating to Server, you DNS Access Control on the settings and registry / script characteristic to be .



iii. **The Disabled Interface Zone Transfers: -** If a defined interface zone ports/physical interfaces will extend and/or A Virtual sub interfaces will extend logical group. The zone firewall security for a flexible layer. Area-based with the safety, this can group administrator Instead, and ports in a policy for each interfaces will extend for the writing of a they implement the policies. Area Transfer between primary and secondary DNS server place. The for specific domain official that need primary DNS servers Upgrade are in the form of qualified DNS zone type that in the files. Secondary DNS server from the server primary DNS these area Read only copy files received and the secondary DNS Servers on the Internet or in the organization to demonstrate improvement DNS Query Is used for [1].

iv. **Enable Dynamic Domain Name System (DDNS) for secure connections only: -**The Dynamic DNS (DDNS) Configure automatic its hostname, Address or other information with active DNS configuration, Often in real time Domain Name System (DNS) , a name Server is a way to update the DDNS and may be a huge boon Upper DNS for administrators to reduce administrative which otherwise in for themselves the hosts DNS resource record need to characteristic.

v. **The Protect / Secure DNS from cache pollution: -**A DNS Cache pollution common problem. The most DNS Server to answer query host before forwarding DNS results of questions are able to cache. A lot in your organization DNS Cache DNS query can improve performance. Problem of entries DNS server cache DNS fake '

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Polluted after users in ', they instead to travel mollified intention web sites can be sent for sites. This DNS converted into IP address domain name on the translation and Tip server takes only a few seconds. But DNS of requests on Number on DNS questions there in the form of millions of processing which is very high results can DNS and other computers slow communication between. , to tackle the problem of speed and for this to speed up the process completed, Cache. Recent DNS Cache reserves questions on local computer result. The repeated this remote DNS reducing the number of questions. It Local cache resolvers known as serving and basic From DNS very rapidly and this local resolver DNS also on Cache Load functions request [1].

Conclusion

This document analyses various the deficiency and secure the attack superficies to your organization localization main DNS server. This expansion also increases in the number of attacks on hosts. The Domain Name System (DNS) internet is one important part. The without internet connection to mostly users / clients to website will not be able. It target of attacks also DNS Server has been to imagine that is not difficult. The System Administrator of continuous their basic structure new lines of defaces to secure there are infrastructure, attackers these invented new generation to undo constantly to search for methods is trying new methods. The number of Internet users in the coming years would be on fast scale is predicted that. Therefore, attackers and also set up vested in DNS system Take advantage of weaknesses and shortcomings can. This kind of time demands this type of place to move to stop attacks that strategic development of technologies. The researchers DNS a system there is a need for fully understand the system and possibly DNS the work was interrupted by new attacks that can should be in search.

Acknowledgement

We would like to thank Prof Dr. Rajesh Kumar Bhagat Head of CSE /IT Department JB Institute of Technology, Dehradun (Uttarakhand) for his immense support and guidance.

References

[1] AvinashKak, “DNS and the DNS Cache Poisoning Attack Lecture Notes on Computer and Network Security”, Purdue University, April 2013
[2] Cyber Security Tip ST04-015 - Understanding Denial-of-ServiceAttacks". United States Computer Emergency Readiness Team.Archived from the original on 2013-11-04. Retrieved December11, 2013.
[3] Classification of Internet Security Attacks (Computing For Nation Development, March 10 – 11, 2011)
[4] Context-aware Clustering of DNS Query Traffic. David Plonka. University of Wisconsin-Madison plonka@cs.wisc.edu. Paul Barford.
[5] DDoS Attack Detection and Attacker Identification International Journal of Computer Applications (BrajeshKashyap, S. K. Jena)
[6] K. Haataja and P. Toivanen. Two practical man-in-the-middleattacks on Bluetooth secure simple pairing and countermeasures.Wireless Communications, IEEE Transactions on, 9(1):384-392,Jan. 2010.
[7] DNS Tunneling for Network Penetration Ghent University, Belgium (Mr.Bjorn De Sutter ,Mr. Bart Coppens and StijinVolckaer)
[8] http://www.verisigninc.com/en_IN/website-availability/ddos-protection/ddos-report/index.xhtml
[9] http://www.stateoftheinternet.com/security-cybersecurity-attack-trends-and-statistics.html