Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 1, January-2021, ISSN 2230-7540

Implementing Zone Alarm Security on DNS Server

Anamika*

Research Scholar, BCA, MCA Persuing PhD (Computer Science), Magadh University, Bodhgaya

Abstract – Any resource or location on the Internet has a unique IP address associated with it. DNS is like a phone book. We remember the phone numbers, or have the numbers on speed dial or saved on our cells etc. of those people who we call frequently. Similarly, in computers (having Windows OS), a HOSTS file works as a speed dial for the computer and directs the computer to the number to be called. But at certain times we need to call someone that is not listed in the speed dial or memory. At such times DNS is very helpful. DNS consists of a vast database of name of servers and their corresponding IP addresses. For example, on typing www.google.com in

The Web browser, the host sends that address to a DNS server. The DNS server then searches for information matching to 'google.com' in its internal database. On matching, it then retrieves the corresponding IP address and sends it back to the computer. The computer then knows where to find the Internet resources

----------X----------

INTRODUCTION ON DNS NAME HIERARCHY

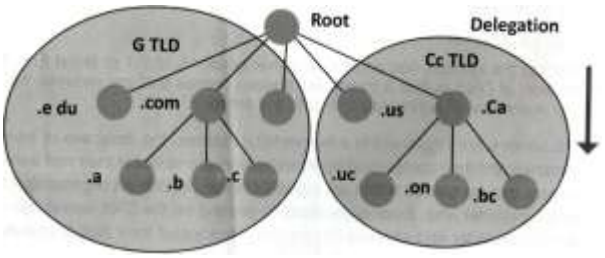
DNS follows a hierarchical name structure. It begins with the root at the top followed by the Top Level Domains (TLDS), then the domain-name and any number of levels each separated with a dot. The root of the tree is represented most of the time as a silent dot ('."). TLDS are split into two types:

Generic Top Level Domains (9TLD)

For example, .com, .eddo, .net, .org, .mil

Country Code Top Level Domain (CCTLD)

For example, .us, .ca, .TV, .up, .in The DNS name hierarchy is shown in the Figure



TYPES OF DNS LOOKUP

Web browsers use DNS to convert Internet domain names to IP addresses. There are two types of DNS lookup:

A) Forward DNS lookup

B) Reverse DNS lookup

The network requests supporting DNS lookups run over TCP and UDP, by default.

A) Forward DNS Lookup

Name-to-address resolution is called as a Forward DNS Lookup which is used by most applications. The user sends a DNS query to resolve the domain name to the Network Security 2014 actual IP address.

B) Reverse DNS Lookup

Address-to-name resolution is referred as Reverse DNS Lookup. They are the exact opposite of the forward DNS lookup. These queries are not made manually by users because the users are more likely to remember host and domain names better than IP addresses. They are used more frequently by computers which prefer numbers. can are commonly required in network-related applications such as server- logging programs and sniffers. But occasionally it is used to determine the domain 109e from where a user its originating. This can be used as a method of authorization.

DNS Zone Alarm Security Issues and Mitigation

DNS servers require some amount of manual maintenance, such as log monitoring and patch

installation are often neglected. And at the same time maintaining authority for domain names and IP addresses is a tremendously important responsibility. Al these factors attract attackers.

Accessing a DNS server offers adequate information about clients that depend and trust on it. DNS poses a security risk if it is not configured properly and also lets out extra information than required. Any information about the network is useful for an attacker; hence keeping this information to a minimum is vital. An attacker attempts to develop a map of the network which can be provided by the DNS server. For example, an attacker may try to perform a zone transfer on a server. This returns all the hosts names and IP address in that particular zone.

Even if the DNS servers block zone transfers by default, it does not stop the attacker from collecting information from the DNS servers. Attackers also use techniques to query a large number of common host names, such as Brute-force guessing the network structure. Therefore, it is important to keep minimum information on the public DNS server.

Denial of Service (DOS) attack is another attack on an organization's DNS server. An attacker, floods a DNS server to use the server's available resources. As a result. it stops responding to the requests. These attacks can be minimized by maintaining a number of servers on separate networks and by isolating the server roles. In this way, an attack on the external servers will not affect the ability to resolve host names internally.

DNS cache positioning is another threat wherein an attacker attempts to trick s DNS server into caching wrong DNS information. The attacker redirects users to a different host. Windows DNS service provides features to block these kinds of attacks but, this service is not sufficient. To prevent these attacks it is best to prevent attackers from accessing the caching DNS servers.

Another threat is that an attacker can break into the DNS server and try te DNS information. Hence, isolating the DNS servers reduces this kind of threat.

DNS Miss-configuration

Following are the effects of DNS miss-configuration:

Service Redirection- A popular location to acquire free and shareware soft applications is download.com. When DNS requests to this site are retirees to the IP address of a malicious attacker's site, the user can download to software without realizing it. The consequences could be huge if the user try the site and does not verify the authenticity through cryptographic signal hashes. The execution of the tainted software can silently install root kits a other backdoors.

A root kit is a type of software. It hides the existence of some processes or programs from normal methods of detection and enables access to a computer.

Fake companies can also use a similar approach to redirect traffic from competitor's Web site to their own. On the other hand, name servers with Mail exchange (MX) records can be modified to redirect email from one domain to another.

A MX record is an entry in a domain name database. It helps to identify the mail server that is responsible for handling emails for that domain name.

Denial of service - The records can be redirected to some nonexistent address like 10.1.1.1. When a record is changed to a nonexistent IP address, every time someone tries to resolve a domain name they are sent to a server that does not exist and hence cannot resolve the name. This results in a denial-of-service attack.

Information Leakage for Recognizance - A significant amount of information about the architecture of a network is maintained by DNS servers. The server naming conventions in many companies give a clear description of the services provided by the server. For example, ns1.company.com is the primary name server while ns2.company.com is the backup. Similarly, mail.company.com is the mail server and www.company.com is the Web server. When trying to get DNS records, the attacker can obtain a complete database of these names along with their associated IP addresses. The database provides sufficient information needed to target specific hosts without actively scanning the network.

Zone Transfer

Automated methods have been introduced to ensure that information across primary.

Recursive Queries

In this case, the client makes a DNS query to the primary DNS server by asking for a correct answer, even if it needs to ask other DNS servers. For example, if the IP address of google.com is asked by the client, then the primary server is not aware and asks another DNS server if it has the information. The primary server returns the answer if it has the information or else asks another server till the time it returns the answer. It's the server's responsibility to provide the information to the client.

In a recursive query, the contacted DNS server will contact other servers on the client's behalf and then return the mapping. In an iterative query, the client asks the server to deliver the mapping only if

it holds it itself. If the server does not have the required address, it replies with the address of another server which the client might try.

Security Threats caused by Recursive Queries

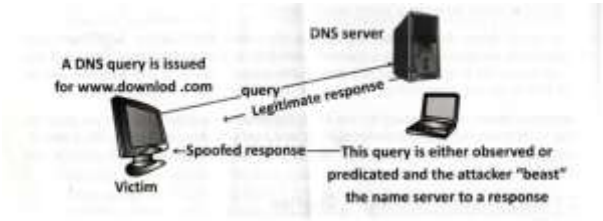
A DNS server supports recursive resolution and it is vulnerable to the security threats such as DNS cache poisoning, DoS (denial of service) attacks, root name server performance degradation, and unauthorized use of resources.

DNS Attacks

Some of the common attacks on DNS are:

DNS Spoofing

The most simple and easy to implement service attack is DNS spoofing as shown in Figure.



DNS Spoofing

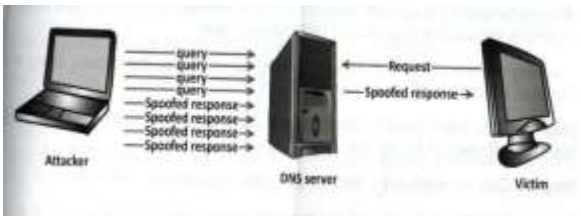
The victim attempts to view the Web site www.download.com. Since the victim has not been to the Web site recently, a cached entry of the IP address does not exist in the client's Address Resolution Protocol (ARP) table. Hence, the victims computer issues a query for www.download.com to its local DNS server.

This DNS query is observed by the malicious attacker and immediately returns a spoofed response to the victim. It is unimportant to identify this traffic on local networks because name servers are widely advertised. All the traffic related to the request travels on UDP port 53. The response from the malicious attacker is received by the victim before the DNS server is able to issue and receive responses from a recursive query to the true authority for www.download.com.

The first response received by the requesting victim is accepted and the secondary response is simply discarded.

Cache Poisoning

Attackers residing on the same local network as the victim are capable to execute imply 'race condition response spoofs to redirect traffic between the attacker and the victim. When the first ARP request is sent, both the victim and the attacker receive the message. The one who replies first will take over the other forever. When attackers fail to reach local servers directly the exploitation method becomes difficult. The most common technique to attack victims in this case is to poison the cache of their DNS server as shown in Figure



DNS Cache Poisoning

Entries in the server have been maliciously modified although the victim continues to trust the responses supplied by the server is called as Cache Poisoning. It is a computer hacking attack in which the data is introduced into a Domain Name System (DNS) name server's cache database. This causes the name server to return an incorrect IP address that diverts traffic to attacker's computer. The first attack became publicly available in 1993. The most difficult attack to prevent against is the birthday attack. This method of DNS cache poisoning launches spoofed DNS queries and requests immediately with a valid user request. As the number of queries reaches 700, the possibility of a collision reaches to 100 percent. An attack is considered 100% successful on reaching around 700 queries. At this point the conventional spoofing attack would only have a success probability of 700 divided by 65535 (1.07%). A collision occurs when the real number that was generated by the server and the guess are the same. This shows that the attacker successfully guessed the query and can spoof the response.

DoS attacks

DoS attacks may occur to servers that support recursive DNS queries These servers are vulnerable to fake requests, which could flood a specific IP address and make the volume of traffic difficult to process.

Securing DNS Server

To secure a DNS server the following factors should be followed:

Use DNS Forwarders

This is a DNS server that performs DNS queries on behalf of another DNS server DNS forwarder offloads processing duties from the DNS server by forwarding the query to the forwarder and benefits from larger DNS cache on the DNS forwarder,

A DNS forwarder prevents the DNS server forwarding the requests from interacting with Internet DNS servers. This helps when the DNS

server hosts the internal domain DNS resource records. Configure the internal DNS server to use a forwarder for all domains for which it is not authoritative instead of allowing the internal DNS servers to perform recursion and contacting DNS servers itself.

Following are the steps to configure a DNS server to use forwarders using the Windows interface in Windows Server 2008:

Step 1- Click Start, point to Administrative Tools, and then click DNS. The DNS Manager will open on the screen.

Step 2 - Click the applicable DNS server in the console tree.

Step 3 - Click Properties on the Action menu.

Step 4 - Click a domain name on the Forwarders tab, under DNS domain.

Step 5 - Under Selected domain's forwarder IP address list, type the IP address of a forwarder, and then click Add.

Note: To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.

Use Caching-only DNS Servers

A caching-only DNS server is not authoritative for any DNS domains. It is configured in such a way that it performs recursion or uses a forwarder. On receiving a response, the caching-only DNS server caches the result and returns the answer to the system by issuing the DNS query to the caching-only DNS server. After some time, the caching-only DNS server collects large cache of DNS responses which improves the DNS response times for DNS clients.

It also improves the security of the organization when caching only servers are used server as their forwarders. The caching-only DNS server performs recursion on Network Security canons response times for DNS clients as forwarders. Internal DNS servers can be configured to use the caching-only DNS behalf of your internal DNS servers.

Protect DNS from Cache Pollution

This is a common problem. DNS server's cache the results of DNS queries before is "polluted" with false DNS entries, then the users are forwarded to malicious Web 5 and not to the sites that they intend to visit. Forwarding the response to the host issuing the query. The DNS cache improves query performance throughout the organization, If the DNS server cache Following are the steps to secure the server cache against names pollution in Windows Server 2008:

Step 1-Open DNS Manager.

Step 2 - Click the applicable DNS server in the console tree.

Step 3 - Click Properties on the Action menu,

Step 4 - Click the Advanced tab. Step 4 - In Server options, select the Secure cache against pollution check box, and then click OK.

Restrict DNS Server to Listen on Selective Addresses

A DNS server service which is performing on a multihued computer is organized in such a way that it can address DNS queries with the help of their IP addresses by default. The user can increase the protection of the DNS server by controlling the IP addresses that are addressed by the DNS server service which is further utilized by DNS clients as a preferred DNS server. Following are the steps to restrict a DNS server to listen only on selected addresses using the Windows interface in Windows Server 2008:

Step 1- Open DNS Manager.

Step 2 - Click the Applicable DNS Server in the console tree.

Step 3 - Click Properties, on the Action menu.

Step 4 - On the Interfaces tab, click only the following IP addresses.

Step 5- In IP address, type an IP address to be enabled for this DNS server, and then click Add

Step 6- Repeat the previous step as necessary to specify other sever IP addresses to be enabled for this DNS server.

To remove an IP address from the list, click it, and then click Remove.

Disable Recursion

All the recursive queries are executed by the DNS server on account of DNS servers and DNS clients who are responsible for submitting the DNS queries to it. This process is performed by default. Recursion can be explained as a name method where the DNS server questions the added DNS servers on account of the requesting client for

determining the name. In the next step, an answer is issued resolution back to the client.

Recursion can be utilized by attackers for refuting the DNS Server service. So, the user is advised to disable recursion on the server if he wants to avoid the Du server which is situated in the network, from accepting the recursive queries.

For performing this procedure successfully, Membership in the Administrators above or corresponding group is essential. Following are the steps to disable recursion o the DNS server using the Windows interface in Windows Server 2008:

Step 1- Open DNS Manager.

Step 2 - In the console tree, right-click the Applicable DNS Server, then click Properties.

Step 3 - Click the Advanced tab.

Step 4 - In Server options, select the Disable recursion check box, and then click OK.

Enable DDNS for Secure Connections Only

Dynamic updates are accepted by many DNS servers. These enable DNS servers to register DNS host names and IP addresses for hosts that use Dynamic Host Configuration Protocol (DHCP) for host IP addressing. Dynamic DNS (DDNS) reduces the administrative overhead for DNS administrators that need to be manually configured DNS resource records for these hosts. DDNS can face a major security issue if they are allowed unchecked. A malicious user configures a machine to dynamically update DNS host records of a file server, Web server, or database server which allows connections that are intended to those servers diverted to the machine. The risk of malicious DNS updates can be reduced by using secure connections to the DNS server to perform the dynamic update. This can be done by configuring the DNS server to use Active Directory integrated zones and using secure d updates. This enables all domain members to dynamically update their DNS Information in a secure context after change is made. Following are the steps to allow only secure dynamic updates using the Windows interface in Windows Server rises 2008:

Step1- Click Start > click Run > type dnsmgmt.msc > press ENTER. The DNS Manager console will open.

Step 2- Click the name of the DNS server you wish to configure in the console tree. Then

open Forward Lookup Zones or Reverse Lookup Zones. ervers

Step 3 - Right-click the name of the zone that you wish to configure, and then click sued Properties.

Step 4 - On the General tab, verify that the zone type is Active Directory-integrated.

Step 5 - Click secure only in Dynamic Updates.

Limit/Disable Zone Transfers

Zone transfers occur between primary and secondary DNS servers. Primary DNS servers are authoritative for specific domains. They contain writable DNS zone files that are updated when required. Secondary DNS servers receive a read-only copy of these zone files from primary DNS servers. Secondary DNS servers improve the DNS query performance in an organization or over the Internet.

Zone transfers are not restricted to secondary DNS servers only. It can be issued by anyone. A DNS query causes a DNS server that is configured to allow zone transfers to dump the total zone database files. Malicious users use this information to explore the naming plan in the organization and attack important services. This can be prevented by configuring the DNS servers to deny zone transfer requests. It can also be prevented by configuring the DNS servers to allow zone transfers only to particular servers in the organization.

Following are the steps to configure zone transfer settings using the Windows interface in Windows Server 2008:

Step 1- Click **Start** > click **Run** > type **dnsmgmt.msc** > press **ENTER**. The DNS Manager console will open.

Step 2 - Click the name of the DNS server you wish to configure in the console tree. Then open **Forward Lookup Zones** or **Reverse Lookup Zones**.

Step 3 - Right-click the name of the zone you wish to configure, and then click **Properties.**

Step 4 - On the Zone Transfers tab, do one of the following:

To disable zone transfers, clear the **Allow zone** transfers check box and the click **OK**,

To allow zone transfers, select the **Allow zone transfers** check box and then do the following:

To allow zone transfers only to specific DNS servers, select Only to the following servers, add the IP address of one or more DN servers, and then click OK,

CONCLUSION:

Advanced Research Projects Agency Network (ARPANET) was the world's Grist wide-area

network created by the United States Defense Advanced Research Project Agency (ARPA) in 1969. It was the world's first operational packet switching network that becomes the global Internet. A flat text file, hosts.txt, was created, to reduce this burden. It contained a listing of server IP addresses and descriptive host names.

A sample of what this would look like as follows:

15.10.9.1 Eric

15.10.9.2 Server

To connect to the system, one could type either telnet 15.10.9.1 or telnet Eric. The main function of DNS is that it translates domain names that are required for the users into numerical IP Addresses to locate the server.

The DNS servers are organized in a hierarchical manner, the database of Internet domain names and their corresponding IP addresses are stored in their root servers. DNS servers can be placed within an organization or outside an organization that is at service provider end. Small organizations depend on the DNS server installed at the service provider end whereas big organizations install their own DNS servers within the site for faster name resolution. This topic focuses on the potential security problems and corresponding possible remedial solution of DNS server.

Some Advanced Techniques for Securing DNS Server

In addition to the methods discussed in the preceding section, there are few more advanced techniques that you can implement for securing a DNS server. These methods are:

1- Using Transaction Signature

2-Using DNS Security Extensions

3-Using Zone Transfer Alternatives

1. Using Transaction Signatures (TSIG)

The DNS works on a question-answer model. If information from the DNS is needed, the client sends a question to a DNS server and the server returns an answer. The server examines a question and determines whether or not to answer it based on the IP address of the client. But this is not ideal. It is considered insecure to authenticate using source IP address alone. Transaction Signatures (TSIG) is an effective way to authenticate DNS. It uses cryptographic signatures for authenticating a DNS conversation. A shared secret is used to establish trust between the communicating parties to ensure that DNS information intending to be from a certain server is actually from that server. Transaction signatures are defined in RFC 2845. TSIG is used by Domain Name System (DNS) to authenticate updates to Dynamic DNS database. However, it can be used between servers and for regular queries. It uses shared secret keys and one-way hashing to give a cryptographically secure way to identify each endpoint of a connection and allow making or responding to DNS update.

2. Using DNS Security Extensions (DNSSEC)

DNS security extensions (DNSSEC) are similar to TSIG. They are designed to provide an authorization method for name server queries. But DNSSEC depends on public key cryptography.

The advantage of using a public key infrastructure is that the configurations can be Manumitted without fear of compromise, and the exploitation of one server does not expose the keys of all servers,

The vulnerabilities that are discovered recently in the DNS combined with technological advances have lessened the time an attacker to hijack any step of the DNS lookup process. By doing this, it takes complete control of a session for example, account and password collection. The only long-term solution to this vulnerability is the end- to-end-deployment of DNSSEC.

DNSSEC protects against attacks by digitally 'signing' the data. This assures that it is valid. To eliminate the vulnerability from the Internet, deploy DNSSEC at each step in the lookup process from root zone to the final domain name. Signing the root is a necessary step in this overall process. This is an important step as it does not encrypt data but attests the validity of the site address that you visit.

DNSSEC creates larger DNS messages and larger zones, which requires additional bandwidth and processing resources.

3. Using Zone Transfer Alternatives

There are many alternatives to conventional zone transfers. One of them is Secure Copy Program (SCP) which is a part of the Open SSH distribution. By default, this program is done manually. It can also be combined with scripts and automated distributed file maintenance methods such as sync and driest.

Using Zone Transfer Alternatives to test it update a zone and see if the slave name server will transfer information. Then change a character of the secret on the master name server, reload the configuration and try to get the slave to transfer the

zone. It should log messages about failed verifications

Use Firewalls to control DNS Access

Firewalls help to control clients who connect to the DNS servers. For DNS servers that are used only for internal client queries, the firewalls block connections frorn external hosts to those DNS servers. For DNS servers that are used as caching- only forwarders, the firewalls allow DNS queries from those DNS servers that use the caching-only forwarders. An important firewall policy setting blocks internal users from using the DNS protocol to connect to external DNS servers.

REFERENCE:

1. Domain Name System (DNS) IANA Considerations, D. Eastlake 3rd (November 2008), Section 3

2. Domain Name System (DNS) IANA Considerations, D. Eastlake 3rd (November 2008), p. 11

3. The Role of Wildcards in the Domain Name System, E. Lewis (July 2006)

4. Global Phishing Survey: Domain Name Use and Trends in 1H2010." Archived 2012-10-03 at the

5. Huston, Geoff (July 2019). "DNS Privacy and the IETF" (PDF). The Internet Protocol Journal.

6. Registration Data Access Protocol (RDAP) Operational Profile for g TLD Registries and Registrars". ICANN. 3 December 2015. Archived from the original on 22 December 2015. Retrieved 18 December 2015.

7. Protalinski, Emil (2010-09-22). "ZoneAlarm caught using fake antivirus scare tactics". Arstechnica.com. Retrieved 2010-11-09.

8. Pegoraro, Rob. "Zone Alarm gives people a new reason to hate security software". Voices.washingtonpost.com. Retrieved 2010-11-09.

Corresponding Author

Anamika*

Research Scholar, BCA, MCA Persuing PhD (Computer Science), Magadh University, Bodhgaya