Fast and Furious DNS Security

By: Shubham Mittal

[http://3ncrypt0r.blogspot.com]

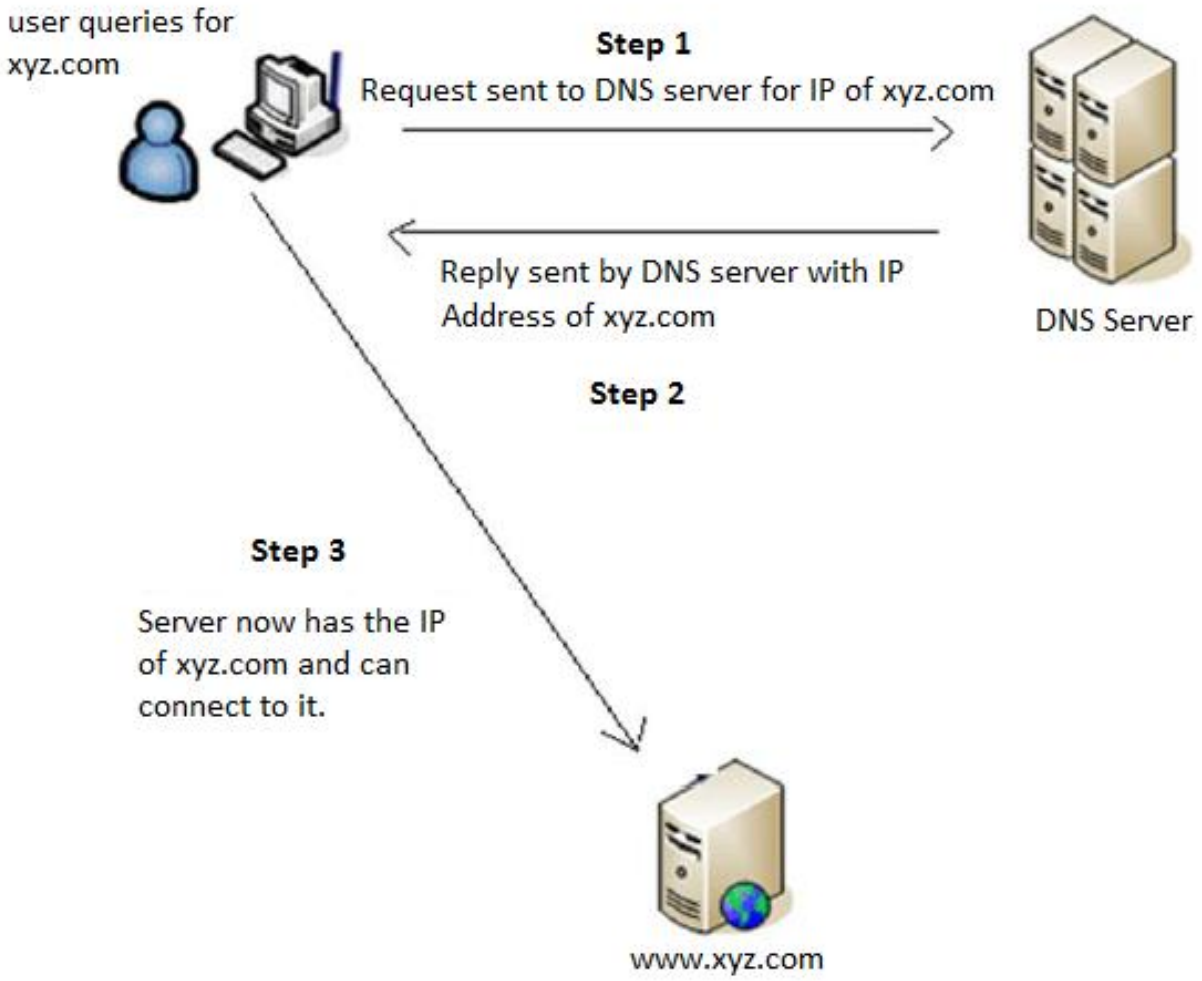
[http://facebook.com/hacktonplanet]

@upgoingstar

Introduction

The Domain Name System (DNS) is a hierarchical, distributed database that contains mappings between names and other information, such as IP addresses. DNS allows users to locate resources on the network by converting friendly, human-readable names like www.microsoft.com to IP addresses that computers can connect to.

An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.xyz.com translates to the addresses 20.52.88.12 (IPv4).



By default DNS works on port number 53 on TCP (Transmission Control Protocol) and UDP (user Datagram Protocol).

Since we have been looking so many DNS attacks getting popular these days, I thought of writing a small paper on Guidelines for Securing DNS Servers so as to make it easy for a Network Administrator to Secure his/her DNS and reduce the chance of getting compromised.

Functions of DNS

DNS is a crucial part of a network and hence securing DNS essentially become quite important. If a DNS is compromised, an attacker can easily prevent normal operations going in the network, can route computers to whatever spoofed IP address or resources he wants, steal information which and a lot of such malicious activity. So first of all, let's first discuss that what are the essential functions of a DNS? (Most of the time, when I ask someone about it, they say: IP to NAME; and NAME to IP. Well, for this reason I am mentioning its functions:

1. DNS is responsible for locating services like DC, etc. for authenticating the services on the network.
2. It is responsible for locating resources like Web Servers, Mail servers, etc. on the network.
3. And obviously, translating Computer names to IP and vice versa.

Possible Attacks (Threats)

So as we are clear with the functions that are performed by DNS, let's understand which of the attacks are possible on DNS.

1. Information Gathering (Reconnainse): Whenever someone asks you what are the common things you do in foot printing; most of the hackers reply with DNS records and zone data. And true indeed. An attacker can easily steal DNS zone data and can enumerate Domain Names, computer names, IP address, etc. which can be used later on to get into the systems.

2. By somehow interrupting the normal process and changing the IP address of legitimates servers (assets), a hacker can redirect the innocent people to his spoofed servers and can control their activities.

3. Another strong chances of attack lies in the DoS attack. A hacker might try to target the availability of a network so that the clients may not be able to obtain name resolution. This can be done by flooding the server with a large number of recursive queries. Eventually the DNS server may become overwhelmed and might be unavailable to the network (clients).

4. A skilled hacker can easily try to use a valid IP address from the DNS zone information in IP packets created by himself only. As these packets will appear to come from a legitimate source on network, this vulnerability can be used for gaining information and compromising other resources. This attack will basically come under Spoofing category.

5. The most famous attack, which is in trend nowadays is DNS cache poisoning. In this attack, additional name resolution information is tried to be returned with a query and the attacker tries to place it in DNS server cache of names and addresses which is not actually authoritative. As client will look for any DNS entries in cache, they might get those fake entries and get redirected to fake Addresses, whereas the attacker will continuously try to poison the cache so as to make the clients redirected for as long as possible. A nice discussion on DNS poisoning and Security was posted on The Hackplanet Blog long ago: http://blog.hackplanet.in/2011/09/small-discussion-on-dns-security.html.

4. Securing the DNS

As lot of attacks are likely to be done on DNS server, we need to place our DNS in a secure place within our network. To be simpler, more easily the asset is available to someone, more easily it is going to be attacked and hence chances for other attacks increase. One of the best ways to help this problem is to introduce a concept of External and Internal DNS servers. For this approach, we have two options:

a. External DNS server being the main server, but the internal DNS will be delegated the control for internal clients, or;

b. Services which need to be accessed publically on the web can be hosted publically (say on ISP), while everything else will be controlled by internal DNS.

4.1 Protecting DNS Zone replication

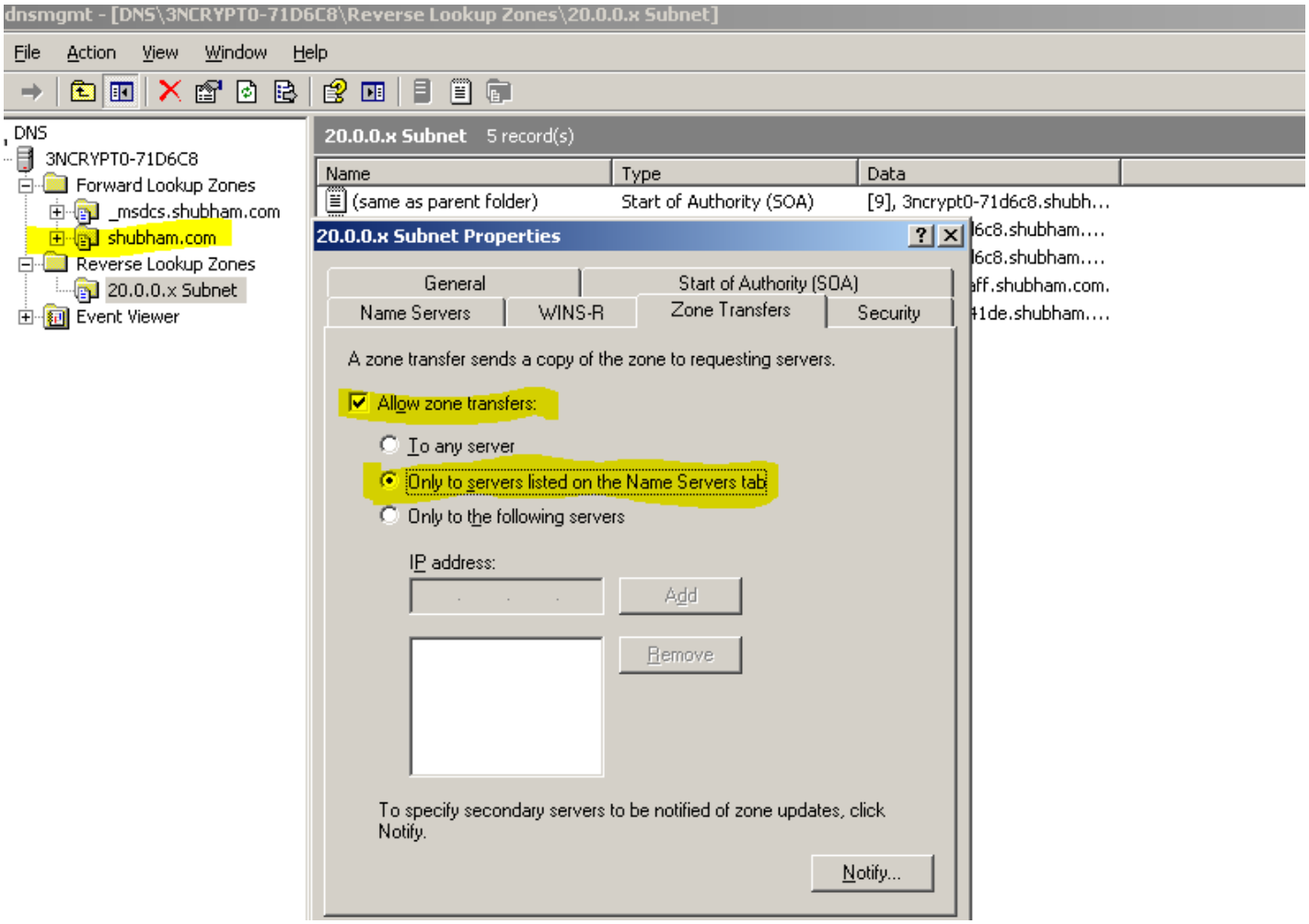
DNS Zone transfers and replication is another issue which is coming in headlines more frequently. Zone replication is basically a service which is required for synchronizing the DNS information between a Primary and Secondary DNS server so that no matter on which machine the changes are applied, they gets reflected on other machine automatically.

Early DNS servers were configured to allow Zone transfers to any DNS servers without proper authentication. However it was realized later on that if internal DNS data was exposed via zone transfer, an internal attacker might use this to find out info about systems on the network. Hence DNS zone transfers must be properly secured. Following are the methods to secure DNS zone transfers for different scenarios:

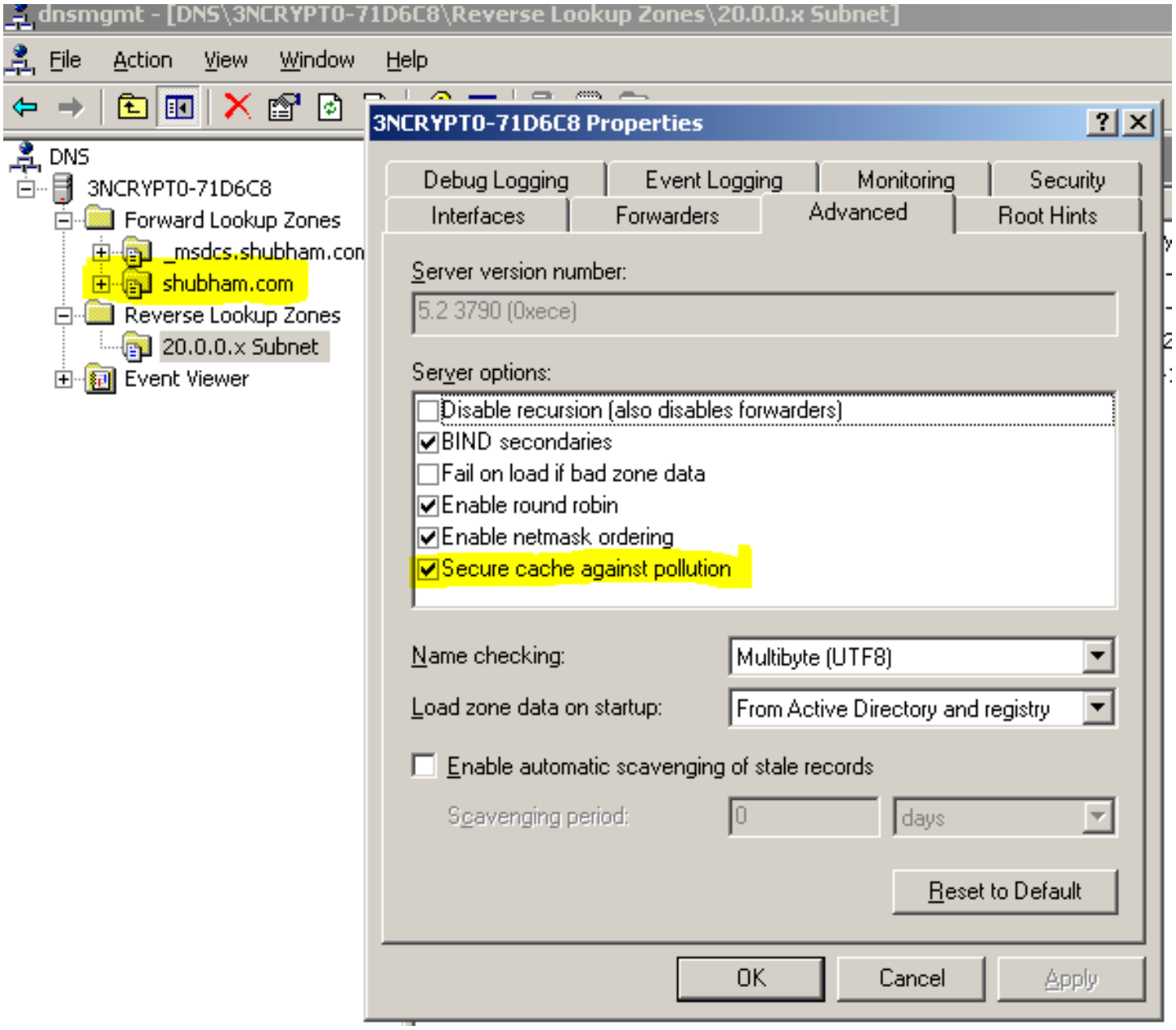
a. **If Active Directory is being used:** If Active directory is implemented on your network, well this is a good news for you. The best way to secure DNS zone transfers on AD is to use Active Directory Replication. This will automatically replicate the information with encryption communication. Also proper

   Authentication between Domain Controllers will happen before any transfer takes place.

b. **If Active Directory is not being used:** If Ad is not implemented or DNS is not integrated with AD, you can simply restrict zone transfers to authorized servers using Zone transfers tab.



4.2 Secure DNS Poisoning (Cache Pollution): As discussed earlier, when a query for name resolution is processed, additional names and IPs are likely to come. In case these are not the legitimate ones, we call it poisoned (polluted). This can be however controlled by using a setting, i.e. “Secured cache against Pollution”. This setting will basically prevent the referral DNS information (which can serve as the malicious one) from being added to cache.



4.3 Secure Dynamic Registration: Any attack on DNS may be an attempt for changing the IP address of a registered service or client. In case the things goes right, every client will be redirected to the spoofed server and can be exploited. This can be protected by using Secure Dynamic Registration, so that the modification of any IP address is already restricted and hence address can't be changed at random.

4.4 Encrypt the Traffic: For whatever data that replicates in the network, all traffic must be encrypted. Two options which can be opted for this includes:

1. Use VPN Tunnel for gateway to gateway encryption between server and routing DNS zone transfer.
2. Create IPSec transport mode policy which can be triggered by communication between primary and secondary servers. This will moreover give you and advantage of authentication.

4.5 Clients must be secured too: For a confidential meeting, we need confidentiality to be maintained by each and every member attending the meet. Similarly, for proper security of a DNS server, we need proper security on the clients. IP address must be specified in DNS itself for making the things simpler.

4.6 Do not rely on DHCP authorization (Secure DDNS only): If you have left your clients to use your DHCP and get DNS information from it, it can be quite troublesome for you. It will simply mean that the security of DNS is directly proportional to security of DHCP. As the DHCP gets compromised, incorrect information can be provided to the clients easily and redirect the clients. These redirection can also be used for DoS attack within the network. We call it secure DDNS, as DDNS is a dynamic update feature enables these DNS servers to register DNS host names and IP addresses for hosts that use DHCP for host IP addressing. However when we are not relying on DHCP, it creates only those Dynamic entries in DNS, which are coming from secure connections and not just from a simple client machine.

4.7 Use Firewall for DNS traffic: Firewalls can also be used in limiting the access to server for only legitimate connections and filtering the connections with malicious intentions. For internal DNS servers, which are supposed to function for only the internal network, we can configure rules on firewall for blocking connections from external hosts. Similarly, configure firewalls for DNS cache-only forwarders, to allow queries from those servers who are actually using cache-only forwarders. Also internal clients must not use DNS protocol to connect to the outside DNS server.

4.8 Secure the DNS file systems: Proper file system permissions must be set on the file system entries related to DNS. Roles must be delegated for this roles so that even a compromise of DNS related account will not result into a complete compromise. Moreover only system account must be given access to %system_directory%\DNS with full permissions so that he can recover whatever situations.

4.9 DNSSEC – DNSSEC stands for DNS Security Extension and is quite known method used to protect users from DNS attacks by detecting the DNS attacks. Everything in DNSSEC is digitally signed. Whenever any data is released, it can be released through authentication only and thus introduces integrity. These messages are also scrambled using a Private Key and is unscrambled using the Public Key. Now as the private key is always unique, you will always be aware of WHO is sending this data. Moreover with this implementation, if the data is changed/modified, the signatures will change leading to the identification of any change. More information about the product : http://www.dnssec.net

4.10 Some other guidelines:

a. Disable recursive Name servers.

b. Use different port number (do not use 53 as fixed by IANA).

c. **Use dnscmd.exe:** Dnscmd.exe can be used at command line or can be incorporated into a script. A simple command for securing DNS will be:

dnscmd /zoneresersecondaries /SecureNS

If you want to switch for secure dynamic update, hit following command:

dnscmd /config /enablednssec 0

d. **Monitor the Logs:** Most of the services on a server create their own logs and these logs are very helpful for providing highly important security information. These can also help Incident handling team for responding to any security incident that has happened in the network.

Log of errors that occur whenever a Net Logon services attempt to dynamically create a DNS record is created in Netlogon.log

e. Ensure that the BIND server is you are using, you are updated with the latest version of the same.

f. **Get an Intrusion Detection System:** always monitor you're the data going through DNS. They key components which are required to be watched are Query/reply rates, Query Types, Data Locality, Caching Memory, Secure Updates, Response time, Search fields, Search time, etc. Monitoring will not alter the attack rates, but undoubtedly give you an aid in identifying and safeguarding more targeted attack vectors with precautionary methods.

g. **And the most important one, KEEP UPDATED with latest attacks and techniques and their countermeasures.**