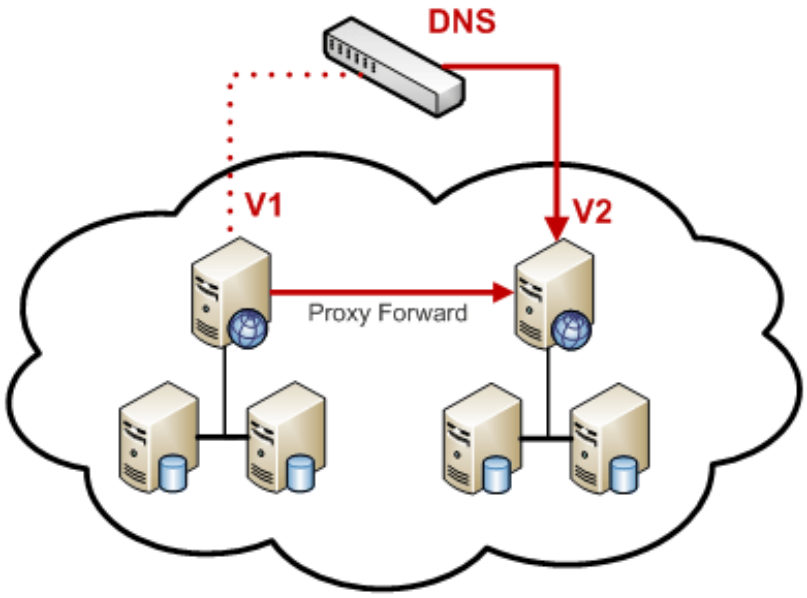
DNS security - Part 1: Issues in DNS security

In this series, I will show you some issues in DNS security and how to secure compromised DNS servers.

In this series, I will show you some issues in DNS security and how to secure compromised DNS servers.



It is undeniable that the importance of DNS for normal network activities for the intranet and the Internet, so detecting problems and finding ways to fix them is a necessity. Here we will go over some general issues for DNS servers:

- DNS zone file compromise
- DNS zone information vulnerability
- Dynamic upgrades are compromised
- Flooding DNS client (denial of service)
- Fake Cache

DNS zone file compromise

The DNS server will be configured on some Windows Server versions. DNS administrators can set up zone configuration and logs using the command line or DNS mmc interface. One of the most common and easiest ways to compromise DNS infrastructure is to directly modify the DNS server configuration or the DNS server itself or from a remote computer.

This type of attack can be done by anyone who has some knowledge of DNS and can access the server. An attacker can sit directly in front of the server screen, connect via RDP or even log in via Telnet. The culprit here may be the person inside the organization or maybe the administrator made a mistake. The security method here is to block the DNS server, only those responsible for accessing the DNS configuration, any remote access method to the DNS server needs to be restricted to real people. necessary.

DNS zone information vulnerability

DNS zone files on the DNS server will contain computer names in that zone, the computer name will be configured manually or configured via dynamic updates. Local network DNS servers often contain the names of all servers on the network (or at least the servers you want to access via name). On the Internet server, usually we just enter the server names we want to access - however some may exist in a location configured by the ISP and one may be in the local network.

Regional information vulnerabilities can occur when an intruder exploits important information about server roles on the network through the names of those servers. For example, if you have a server that is accessible via the name PAYROLL, this information will be very valuable to the attacker. This is something we can temporarily call 'traces'.

An attacker can exploit the names of other computers on the network using a variety of methods. For example, if all roaming machines are allowed, the intruder can download the entire regional database to his computer through roaming. Even without roaming, an attacker can take advantage of reverse DNS queries to detect the computer name in the network. From there they can create a comprehensive network diagram from this DNS data.

In addition, the intruder can gather information and determine which addresses are not used in the network. Then use these unused addresses to set up a fake DNS server, which is because in some cases, network access control is set for all network IDs or certain IDs instead of separate IP addresses.

Finally, a common practice in DNS hosting of small businesses (where hosting private DNS services) is to combine private and public areas on the same DNS server while the DNS infrastructure is seperate. In this case, you will expose both internal and external names in the same area, which allows an attacker to easily find the internal address space and naming agreements. Normally, they will have to break into the network to discover the internal area information, but when the same server hosting both general and private information on the same DNS server, the attacker will now have the opportunity. Great to attack you.

Dynamic upgrades are compromised

DNS dynamic updates are convenient for DNS administrators. Instead of having to manually create records for all clients and servers, all you need to do now is enable dynamic DNS updates on both the server and the client. When using a Windows DNS client and server, you can configure DHCP to support dynamic DNS upgrade. With this dynamic upgrade, simply turn on the function and let the computers register themselves in DNS; You do not need to manually create DNS records.

Obviously everything has its price and in this case, this convenience also entails a hidden security risk for dynamic DNS. There are many ways to perform these dynamic DNS updates, which can be classified into two areas: safe and unsafe upgrades. For secure updates, the client system needs to be authenticated (for example, using a computer account contained in Active Directory) before it can upgrade itself. Unsafe updates appear when you allow any host to register its address in DNS without requiring authentication.

However, safe dynamic upgrades are not all the same. For example, if you restrict only administrators or security administrators to join the domain, then dynamic DNS updates are quite safe in the Windows environment. However, if you allow anyone to join their computer to the domain, the security issue here will be greatly reduced.

When dynamic updates are compromised, an attacker can change the information in the log so that computer names will be redirected to the servers the attacker sets up to achieve their goals (for example, like loading malicious software into a computer to make it a part of the botnet that the attacker is controlling. Another problem an attacker can do in this situation is to perform a simple denial of service attack by deleting the main record, such as records for DNS servers or domain controllers.

Deny DNS service by flooding the client

Speaking of DoS, if you've never encountered this type of attack, consider it a blessing to you. Because DNS queries are not verified, the DNS server always tries to answer the queries it receives. This means it is very easy to perform a denial of service against a DNS server. There are many botnets that can create DDoS attacks to disable DNS servers long enough for an attacker to set up a fake DNS server to answer queries. Users have no way of knowing if the new DNS server is a fake server, they will be redirected to the attacker's server. These sites are often designed to resemble real sites and use the trust of users on real sites to increase access to personally identifiable information, and then perform such attacks.

Spoof cache

This DNS server will query another DNS server for information. To improve performance for the entire DNS infrastructure, DNS servers will store query results for a period of time before the records to provide name resolution. If the second query has the same name before the timeout, the DNS server will respond to the information it saved in the DNS cache instead of the query to another DNS server.

While it can significantly improve overall performance, this approach causes a security hole. Security vulnerabilities exploited here called 'DNS cache poisoning' mean DNS spoofing. DNS spoofing takes place when the DNS server sends a query to another DNS server and the DNS server returns incorrect information. In most cases, the DNS server returns false information that the servers have been compromised.

Cache spoofing can occur because DNS servers do not check the validity of responses, nor do they verify the responses they receive from other DNS servers. The 'guest' DNS server will receive the information in response and save that information, then provide false information to the servers configured as the server's DNS client.

Conclude

In this article, I have discussed some of the issues in DNS security and how to secure compromised DNS servers. In Part 2, I will take a closer look at some tips to improve DNS security and take a closer look at security features in Windows Server 2008 and DNSSEC. We will also configure a secure area using DNSSEC and consider how to use DNSSEC to improve DNS security for the organization.