Global Information Assurance Certification Paper

Implementing and Securing DNS on Microsoft Windows NT Server

For

By
Corey White

TABLE OF CONTENTS

1.0 Introduction

The purpose of this document is to demonstrate the secure way to implement DNS on Windows NT. There are many documents on this subject written for the BIND implementation on UNIX, but not many for DNS on Windows NT. Many corporations' IT staff are not experienced with UNIX these days, therefore many enterprise level DNS implementation are implemented on Windows NT.

2.0 DNS Security Policy

Before implementing any new network device the security policy must be updated. Policies and procedures must be written to ensure that the level of security does not decrease just because the DNS server administrator left the company. The security policy and procedure states:

- Who is allowed to administer the DNS server?
- How new DNS records are added
- How often the DNS server is backup
- How often virus software is updated

In a separate document there should be an "as built" document detailing how the server is configured and how DNS is designed as a whole. This is an important document to have in case the server has to be rebuilt from scratch by someone other that the person than originally built it or for simple troubleshooting.

How to write a security policy is another topic in itself and has already been addressed by SANS. For the purpose of this document I just wanted to address the fact that the DNS server should be part of the your companies security policies and procedures for the administration for the DNS server should be thoroughly documented. A link to the SANS sample security policy is listed below:

http://www.sans.org/newlook/resources/policies/policies.htm

2.1 The DNS Server Administrator

The Administrator of the DNS server must thoroughly understand DNS before implementing it or the DNS servers could be subject to misconfigurations that can be exploited by hackers. The administrators' duties relating to DNS server should be well documented in the corporate policies and procedures.

3.0 The DNS Server Installation and Configuration

Let's get started with the DNS server itself. First the Windows NT server has to be built. The basics of installing Windows NT are not going to be covered here. It

is assumed that that the software is already properly installed. The most important part of building the server is applying the latest service pack for your version of Windows NT whether it is 4.0 or 2000. The latest service pack can be found at the following url:

http://www.microsoft.com/ntserver/

There are also many hot fixes and patches that come out for Windows NT therefore, Microsoft's website must be monitored frequently for new security vulnerabilities. If it is not convenient to keep checking Microsoft's website then you can subscribe to their email list for new vulnerabilities. The email updates allow for administrative to maintain a secure Microsoft network with less effort. A link to the email notification web page is listed below:

http://www.microsoft.com/technet/security/notify.asp

3.1 Configuring DNS on NT

The actual configuring DNS on Windows NT is not difficult and there is perfect book by O'reilly for this purpose. The link for this book can be found below:

http://www.oreilly.com/catalog/dnswinnt/

The purpose of this document is to ensure the server is secured once DNS is installed on Windows NT.

3.2 Hardening the Windows NT Server

The Windows NT Server must be security hardened, because by default (out of the box) it is not secured. The default configuration for a Windows NT Server is extremely user friendly to the end user and to hackers; therefore it is imperative that the server be security hardened. Microsoft has it's own hardening recommendations that come in the form of a checklist that can be downloaded and followed. The link below is to Microsoft's hardening checklist:

http://www.microsoft.com/technet/security/tools.asp

There are many other hardening documents or checklist that can be used to secure a Windows NT Server. SANS offers another great checklist that can be used for hardening Windows NT. The link below is to SANS hardening checklist:

http://www.sans.org/giactc/nt_sbs_info.htm

4.0 Server Redundancy

Redundancy is very important for any DNS implementation. As we all know DNS resolves names to IP addresses which is an extremely important function to many organizations. So many applications rely on DNS to work properly. A few applications that rely on DNS are http, smtp, and any other application that require the Fully Qualified Domain Name (FQDN).

A redundant design should include at least two internal DNS servers dependent on the size of the organization. If a large corporation is involved, then DNS servers should be distributed throughout the company. DNS clients should not have to travel over slow WAN links to resolve a name. Slaves servers can be setup on the local DHCP/WINS server at each site. This will allow for local resolution of most DNS names in its cache. At each site there should be at least two DNS/DHCP/WINS servers configured in a locked room with limited access.

Many large corporations have specialized software for the management and security on DNS/DHCP/WINS one such product is QIP. QIP is the number one ranked IP address management software on the market. More information on QIP can be found at the following url:

http://www.quadritek.com/

5.0 DNS Design Redundancy

A recent DoS attack on Microsoft DNS servers in February 2001 is because of poor DNS Design. Next we are going to briefly explain what happened to Microsoft's DNS server and how to avoid it. As you can see below the output from Domtols.com shows the Microsoft had many DNS servers to resolve from, but they were all located at Microsoft and on the same subnet. So if a hacker is able to flood traffic to that subnet, then no one will be able to resolve DNS names for any of Microsoft's domains hosted by these servers.

Output from Domtools.com Nslookup:

dns1.tk.msft.net.
dns2.tk.msft.net.
dns3.tk.msft.net.
dns4.cp.msft.net.
dns4.tk.msft.net.
dns5.cp.msft.net.
dns6.cp.msft.net.
dns7.cp.msft.net.

Microsoft was able to fix this problem by implementing more DNS servers hosted by Akamai as you can see below:

Output from Domtools.com Nslookup:
dns1.tk.msft.net.
dns2.tk.msft.net.
dns3.tk.msft.net.
dns4.cp.msft.net.
dns4.tk.msft.net.
dns5.cp.msft.net.
dns6.cp.msft.net.
dns7.cp.msft.net.
z1.msft.akadns.com.
z2.msft.akadns.com.
z6.msft.akadns.com.
z7.msft.akadns.com.
dns.cp.msft.net.

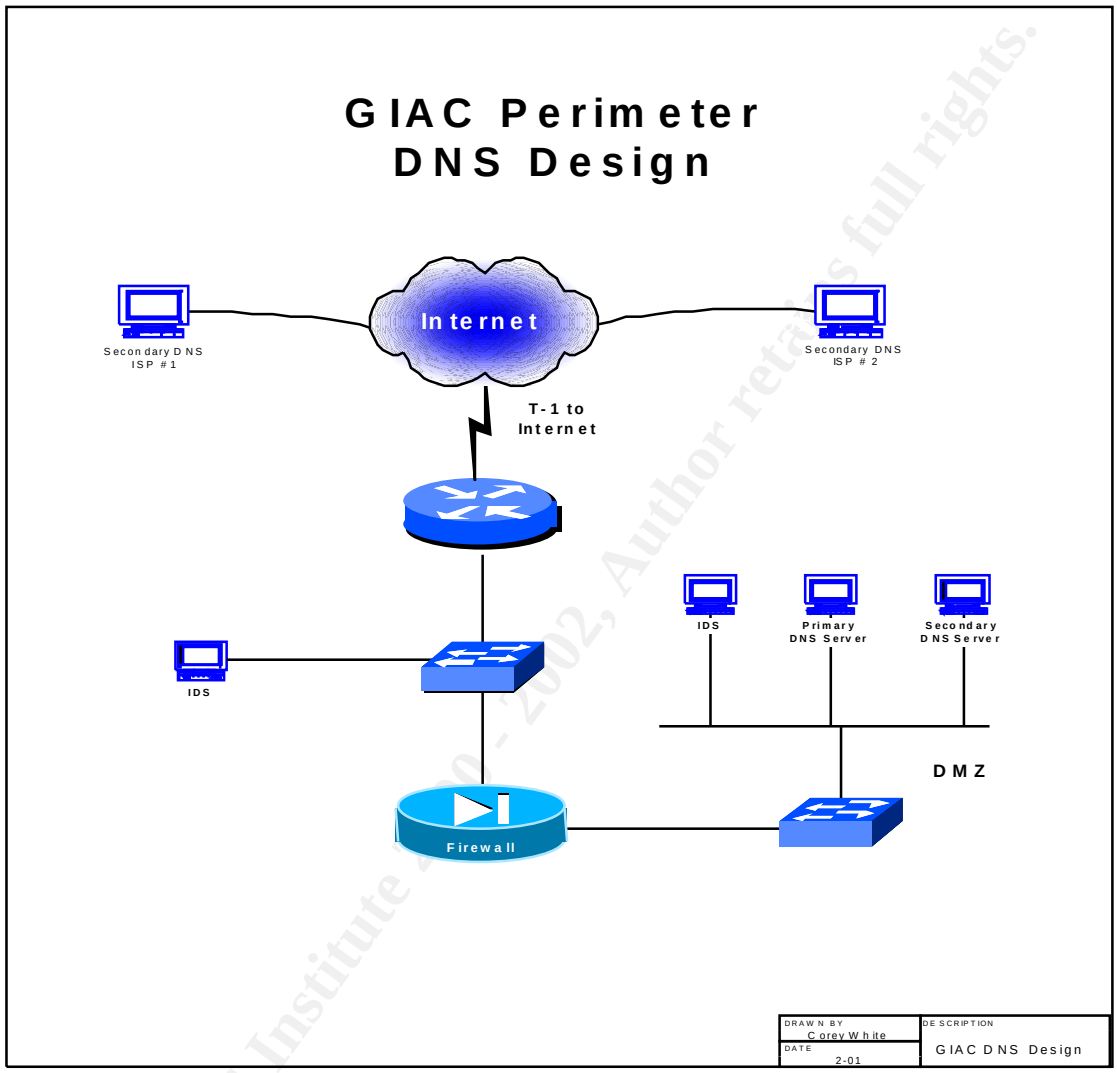
For a hacker to launch a DoS attack on Microsoft's DNS they now have to bring all the above listed servers down or make them available. The servers are now on different subnets making it even more difficult to bring the site down. In my opinion they should have at least 3 different ISPs or hosting companies hosting their DNS distributed throughout the world to ensure this can not happen again.

According to a recent survey conducted by Men and Mice, 38% of Internet Domains share Microsoft's DNS vulnerability. I am sure in the future we can look to see more attacks on this type.

5.1 DNS Design

A DNS design consists of one primary (master) and multiple slaves. The most important part of any DNS design is who owns the primary. You should house your DNS server yourself. You should not trust someone else to properly secure you DNS server. If you are forced to trust someone else make them agree to a SLA (Service Level Agreement) stating that the DNS server will be properly secured behind a firewall or whatever your security policy states.

The diagram below shows a DNS design for hosting your external domain (Domain with and Internet presence, not the Intranet). A router and a firewall should protect the primary server, as shown below. The DNS server located behind the firewall is authoritative for the domains it is hosting. This means that all changes are made on the primary and are pushed out to the secondary servers.



5.2 Split DNS Design

Split DNS is the design of separating the internal DNS servers from the external DNS servers. The data in these servers should be completely different. The internal servers only contain internal DNS entries and the external server only contains external entries. Hackers love to find DNS servers that are not split and expose internal host to the Internet. They can use this information to get the IP address of internal hosts and find out specific information about the internal configuration of the network. If an attacker can see an hostname called fw01, he can easily assume it is a firewall and begin attacking it for vulnerabilities. The attacker may not have known the IP address of the firewall because ping usually is disabled by the firewall. But now the attacker knows the IP address of the firewall and many other network devices, that he can now launch attacks against.

6.0 ISP Selection

When selecting an ISP to host you secondary DNS server, you should ensure that that they are security conscious and not some mom and pop shop that does not have any idea about security. You should interview the ISP about their infrastructure and how the DNS should be secured. Their policies and procedures should be made available to you to ensure that your server is managed properly. If they don't have policies and procedures or adequate security you should force them to use your policies and procedures and make them sign a SLA. The SLA will protect your organization from possible financial loss due to the ISPs lack of security. If your ISP will not agree to these terms, take your business elsewhere.

If Microsoft had an outside ISP when the DoS attack was launched, they could have sued the ISP for their losses or the ISP would have to pay a set amount stated in the SLA.

6.1 ISP Service Levels Agreements

A services agreement should be established to ensure that the DNS data that is hosted by the ISP is properly secured. The SLA should include the following:

- The DNS server should be protected by a firewall
- Ping and trace route should be disabled to the server
- The DNS server should be logged monitored and audited for security incidents
- The server platform should be hardened & secured
- Zone transfers should not be allowed except from secondary server

7.0 Firewall Configuration

The following sections give details on how to secure a DNS implementation using firewalls and router ACLs.

7.1 Firewall Configuration

Network Address Translation (NAT) should be used on the DMZ where the DNS server is located to further protect it from hackers. DNS traffic should be the only traffic allowed to the DNS server, which is TCP (zone transfers) and UDP port 53 (DNS queries). Outside traffic should not be allowed to the DNS server except authorized DNS traffic.

7.2 Router Configuration

Two lines should be added to the access-list to allow TCP and UDP port 53 to access the IP address of the DNS server.

7.3 Log Monitoring (IDS, Firewall, and DNS)

Proper logging is essential to any security implementation and should be implemented on the DNS server, the firewall and the Internet router.

To receive the benefits from above listed logging, the logs have to be monitored for an suspicious traffic. If they are properly monitored, the chances of intruders penetrating the security measures implemented decreases.

7.4 Service Packs and Patches

The latest vendor patches and updates for the Firewall and router should be regularly monitored and installed, if necessary to ensure that the proper security levels are maintained.

7.5 General Security Concerns

This section lists general security related to DNS that should be addressed:

- Do not configure the HINFO information because it reveals too much information about the server platforms to the outside world.
- Clean out all test records that are not needed hackers zero in on these records because they are not usually well secured. At this point the hackers knows the IP address of the box and can now launch attacks against it.
- Restrict zone transfers using the notify option on Microsoft's DNS only to slave (secondary) servers.

References

Domtools.com , DNS Utilities , Paul Balyoz. 10 February 2001. URL: http://www.domtools.com. 10 February 2001

DNS Security, Men & Mice. Thoroddsstadir vSkogarhlid. 10 February 2001. URL: http://www.menandmice.com/index.htm

Securing an Internet Name Server. Cricket Liu. 10 February 2001. URL: www.acmebw.com. 10 February 2001

DNS on Windows NT By Paul Albitz, Matt Larson & Cricket Liu. 1st Edition October 1998 1-56592-511-4,

Implementing DNS on NT. Bill Gates, May 1997. URL: Www.microsoft.com/technet