DoS Attacks on DNS Server Infrastructures
Stan Wisseman
15 February 2001

1 Introduction

This paper is written to fulfill the practical assignment of the GIAC LevelOne Security Essentials certification from the SANS Institute.

Microsoft's reputation suffered again by what officials describe as a DoS attack. Apparently, the crackers took advantage of security glitches resulting from a Microsoft technician's blunder [11]. While Denial of Service (DoS) attacks are not considered sophisticated, the recent shutdown of Microsoft Web sites through use of DoS attacks on their DNS servers (rather than their Web servers) may be a beginning of a new wave of attacks against vulnerable DNS server infrastructures.

Defense-in depth won't prevent this attack. Even if your Web servers are in tip-top shape, the firewalls are doing their job, and your backend application servers and databases are in perfect order, none of this matters if an attacker manages to take out your DNS servers. Without DNS servers, no one on the Internet will be able to find your servers [10]. To see a Fortune 100 company such as Microsoft suffer a multi-day outage because its DNS infrastructure was not up to the task is disturbing indeed.

2 DNS and DoS Attacks

DNS (domain name system) servers are analogous to an Internet business phone book: They translate computer names into the numbers that are needed to actually access the computer. For example, it maps names such as www.securityportal.com to IP addresses such as 209.67.74.22. Without your DNS servers, internal services may not work properly, email deliveries can fail, and access to servers will time out as DNS queries fail Given the importance of DNS servers, attacks on them are common [6, 7, 8]. What appears to be different in this Microsoft incident was that a *DoS attack* was used to target Microsoft's DNS servers.

In a DoS attack, one system typically uses source facilities to overwhelm a single destination system [4, 5]. All the source of the attack has to do is overwhelm any of the previously mentioned in-path components and the attack is considered successful, as it will cause the attempted legitimate connections to fail due to timeouts. The effects of this type of attack can be devastating for a company that lives and dies by network access.

A Distributed DoS (DDoS) attack is much more intense and damaging than a normal DoS attack. DDoS attacks are designed to overwhelm a target system through continuous traffic loading to the target system from multiple sources at the same time. In early February 2000, DDoS and smurf attacks where launched on several high profile sites (e.g., Yahoo, Buy.com, CNN.com, Amazon.com).

DoS attacks aren't especially new in Internet terms. This form of attack is considered to be the province of "script kiddies," relatively unskilled youngsters who have just enough technical knowledge to follow instructions on how to attack networks. As a result, systems administrators have often downplayed them as adolescent bids for attention.

3 Attack Against Microsoft's DNS Servers

Unlike the DDoS attacks last February, the hack that all but erased Microsoft's Web presence went after the company's Internet routers, not its Web servers. Web performance management services company Keynote Systems, which monitors Microsoft's and many other companies' Web sites, reported a noticeable downgrade in performance the morning of 25 January on Microsoft's Expedia.com site, which dropped to a 55 percent success rate, or the rate at which pings sent by Keynote can access the site. The downgrade spread to MSN.com shortly after that and by late morning Pacific Time, both sites were down to a 1.5 percent success rate, according to Keynote, of San Mateo, Calif [1].

As it turns out, the DNS records for MICROSOFT.COM show that the primary and secondary name servers are, in fact, one and the same. This is contrary to all established standards for a robust DNS infrastructure [8]. Most likely the chokepoint router was targeted by the crackers, which would have had the effect of blocking access to the four DNS servers behind it. It doesn't matter how powerful and fast and well secured those four DNS servers were; the router in front of them was most likely dead (traceroute response was very sporadic) [10].

Microsoft's practice of staying silent until -- and if -- it's ready to speak angered many who felt that they'd been left to pick up the pieces this week after the software giant took a tumble [3]. ISPs, company support desk personnel, and almost anyone who seemed they might know what was going on were besieged with phone calls and e-mails.

4 Breadth of Vulnerability

This type of hack is more difficult to identify and defend against than a standard DoS attack. Instead of receiving the tell-tale flood of packets and huge consumption of bandwidth that signal a DDoS attack, the target company's Web servers operate normally during this kind of event. Indeed, Microsoft said at several points Thursday afternoon that it was not having any problems with its sites [1].

SecurityPortal.com posted the following table listing public information about several major companies' DNS configurations [10]. This information was gleaned by using:

```
whois example.org@whois.someprovider.com
dig -t ns example.org
traceroute foo.example.org
```

Name	traceroute results	Comments
Caldera	Both pass through 208.46.255.178 (1 and 2 more hops)	One site with a chokepoint router, vulnerable to attack.
Debian		Well distributed servers.

FreeBSD		Very well distributed servers on major links/systems
IBM		Very well distributed servers on major links/systems
Kernel.org	Both pass through 209.10.12.53 (2 and 3 more hopes)	Probably one site with a chokepoint router, vulnerable to attack., would also affect transmeta.com
Mandrake	Both pass through 209.244.10.46	One site with a chokepoint router, vulnerable to attack.
Microsoft	DNS*.CP..MSFT.NET servers pass through 207.46.190.117	
NetBSD		
Novell		
OpenBSD		
Red Hat		
Sun		
SuSE	*.SUSE.COM servers pass through 198.32.128.81	

Name	Servers by whois listing	Servers by dig -t ns
Caldera	NS.CALDERASYSTEMS.COM 216.250.130.1 NS2.CALDERASYSTEMS.COM 216.250.130.254	NS.CALDERASYSTEMS.COM 216.250.130.1 NS2.CALDERASYSTEMS.COM 216.250.130.254
Debian	SAMOSA.DEBIAN.ORG 209.249.97.234 SAENS.DEBIAN.ORG 216.66.54.50 NS1.LDSOL.COM 62.161.210.241 NS2.CISTRON.NL 195.64.68.28 OPEN.HANDS.COM 195.224.53.39	SAMOSA.DEBIAN.ORG 209.249.97.234 SAENS.DEBIAN.ORG 216.66.54.50 NS1.LDSOL.COM 62.161.210.241 NS2.CISTRON.NL 195.64.68.28 OPEN.HANDS.COM 195.224.53.39

FreeBSD	NS1.ROOT.COM 209.102.106.178 WHO.CDROM.COM 204.216.27.3 NS1.CRL.COM 165.113.1.36 NS2.CRL.COM 165.113.61.37 NS1.IAFRICA.COM 196.7.0.139 NS2.IAFRICA.COM 196.7.142.133	NS1.ROOT.COM 209.102.106.178 WHO.CDROM.COM 204.216.27.3 NS1.CRL.COM 165.113.1.36 NS2.CRL.COM 165.113.61.37 NS1.IAFRICA.COM 196.7.0.139 NS2.IAFRICA.COM 196.7.142.133
IBM	NS.WATSON.IBM.COM 198.81.209.2 NS.ALMADEN.IBM.COM 198.4.83.35 NS.AUSTIN.IBM.COM 192.35.232.34 NS.ERS.IBM.COM 204.146.173.35	NS.WATSON.IBM.COM 198.81.209.2 NS.ALMADEN.IBM.COM 198.4.83.35 NS.AUSTIN.IBM.COM 192.35.232.34 NS.ERS.IBM.COM 204.146.173.35 INTERNET-SERVER.ZURICH.ibm.com 195.212.119.252
Kernel.org	NS2.KERNEL.ORG 209.10.41.242 NS1.KERNEL.ORG 209.10.217.83	NS2.KERNEL.ORG 209.10.41.242 NS1.KERNEL.ORG 209.10.217.83
Mandrake	MOSEISLEY.MANDRAX.ORG 63.209.80.226 DAGOBAH.MANDRAX.ORG 63.209.80.227	MOSEISLEY.MANDRAX.ORG 63.209.80.226 DAGOBAH.MANDRAX.ORG 63.209.80.227
Microsoft	DNS4.CP.MSFT.NET 207.46.138.11 DNS5.CP.MSFT.NET 207.46.138.12 DNS6.CP.MSFT.NET 207.46.138.20 DNS7.CP.MSFT.NET 207.46.138.21 Z1.MSFT.AKADNS.COM 216.32.118.104	DNS4.CP.MSFT.NET 207.46.138.11 DNS5.CP.MSFT.NET 207.46.138.12 DNS7.CP.MSFT.NET 207.46.138.21 DNS6.CP.MSFT.NET 207.46.138.20 Z1.MSFT.AKADNS.COM 216.32.118.104 Z2.MSFT.AKADNS.COM 32.96.80.17 Z6.MSFT.AKADNS.COM 207.229.152.20 Z7.MSFT.AKADNS.COM 213.161.66.158
NetBSD	NS1.BERKELEY.EDU 128.32.136.9 NS2.BERKELEY.EDU 128.32.136.12 UUCP-GW-1.PA.DEC.COM 16.1.0.18 UUCP-GW-2.PA.DEC.COM 16.1.0.19	NS1.BERKELEY.EDU 128.32.136.9 NS2.BERKELEY.EDU 128.32.136.12 UUCP-GW-1.PA.DEC.COM 16.1.0.18 UUCP-GW-2.PA.DEC.COM 16.1.0.19
Novell	NS.NOVELL.COM 137.65.1.1 NS.UTAH.EDU 128.110.124.120 NS1.WESTNET.NET 128.138.213.13	NS.NOVELL.COM 137.65.1.1 NS.UTAH.EDU 128.110.124.120 NS1.WESTNET.NET 128.138.213.13

OpenBSD	ZEUS.THEOS.COM 199.185.137.1 CVS.OPENBSD.ORG 199.185.137.3 NS.SIGMASOFT.COM 198.144.202.98 CS.COLORADO.EDU 128.138.243.151 NS.EUNET.CH 146.228.10.16	ZEUS.THEOS.COM 199.185.137.1 CVS.OPENBSD.ORG 199.185.137.3 NS.SIGMASOFT.COM 198.144.202.98 CS.COLORADO.EDU 128.138.243.151 NS.EUNET.CH 146.228.10.16
Red Hat	NS1.REDHAT.COM 199.183.24.210 NS2.REDHAT.COM 216.148.218.250 NS3.REDHAT.COM 63.240.14.66	NS1.REDHAT.COM 199.183.24.210 NS2.REDHAT.COM 216.148.218.250 NS3.REDHAT.COM 63.240.14.66
Sun	NS.SUN.COM 192.9.9.3 NS-BRM.SUN.COM 192.18.99.5 NS.USEC.SUN.COM 192.9.48.3	NS.SUN.COM 192.9.9.3 NS-BRM.SUN.COM 192.18.99.5 NS.USEC.SUN.COM 192.9.48.3
SuSE	NS.SUSE.DE 194.112.123.193 NS1.SUSE.COM 202.58.118.2 NS2.SUSE.COM 202.58.118.4	NS.SUSE.DE 194.112.123.193 NS1.SUSE.COM 202.58.118.2 NS2.SUSE.COM 202.58.118.4

As was noted in [10], two vendors stand out as having particularly poor DNS infrastructures. Caldera maintains by far the worst, with only two DNS servers hosted at the same site. In fact, this is the site that hosts most of their servers, email, FTP and so on. Essentially, they have a network link to their offices with all of their infrastructure based there. If someone were to flood a router on that link, they could likely take out Caldera entirely — DNS, email, secondary email, FTP, etc.

Mandrake is another vendor with a poor DNS infrastructure. While not nearly as bad as Caldera's, Mandrake's is far from perfect. Mandrake appears to host two DNS servers with Level3, and it appears that they are not firewalled from the Internet. Thus an attack on the DNS servers themselves is possible.

5 Countermeasures

National or global organizations should, as standard operating procedure, have several DNS servers (you can register up to six) on different networks served by different ISPs and running on different operating systems -- Solaris and FreeBSD, or Linux and HPUX -- so as to minimize the threats for DoS attacks, known OS vulnerabilities, and connectivity issues [8, 9]. This is your first line of defense against an attacker. Since hopefully no attacker will be able to take out all the root servers, you can use them to do limited load balancing, but more importantly, to list multiple servers [10].

However, if all your DNS servers are running at 100% capacity and an attacker takes one server out, the reduction of a single DNS server may cause enough added load on the other servers to make them unresponsive. Ideally, a single DNS server should be able to handle the full load. Realistically, you should be able to lose at least one, and probably two servers without overloading the remaining ones.

Some companies already offer supra-reliable DNS to nervous customers worried about downtime. Nominium, a Redwood City, Calif. startup, boasts it has many collections of DNS servers, each with at least two different hardware and OS platforms, and each connected to two different ISPs.

6 Summary

Even if you are a technically competent organization, your business is at significant risk without a highly reliable DNS infrastructure. It doesn't matter where the problems come from, you have to follow best practices in terms of having redundancies for when systems fail and monitoring to catch problems early and correct them.

This is not a network task that should be put off. If you do not have DNS servers in at least two (or preferably three or more) separate locations, then you should start on this immediately. While it may not be advisable to completely outsource your DNS (the provider may not have properly secured DNS servers), co-locating machines at a major co-location provider is a reasonable solution [10] For most organizations, the cost to host several machines is minor compared with the cost of having an extended outage.

7 References

The following are cited as references for this paper:

[1] Callaghan, Dennis and Fisher, Dennis. Beware of Brainier Web attacks! 26 January 2001. http://www.zdnet.com/zdnn/stories/news/0,4586,2679094,00.html?chkpt=zdnn_rt_latest

[2] Delio, Michelle. Microsoft Crashes: The Fallout. 26 January 2001. http://www.wired.com/news/infostructure/0,1377,41454,00.html

[3] Delio, Michelle. Microsoft: Silence of the Flacks. 26 January 2001. http://www.wired.com/news/business/0,1367,41435,00.html

[4] Fuller, Edward. Denial of Service Attack. 6 April 2000. http://www.sans.org/infosecFAQ/securitybasics/dos.htm

[5] Hancock, Bill, PhD. Network Attacks: Denial of Service (DoS) and Distributed Denial of Service (DDoS). http://www.exodus.com/information/ddos/index.html

[6] Hanley, Sinead. DNS Overview with a Discussion of DNS Spoofing. 6 November 2000. http://www.sans.org/infosecFAQ/DNS/DNS.htm

[7] Holland, Jeff. DNS Security. 23 July 2000. http://www.sans.org/infosecFAQ/firewall/DNS_sec.htm

[8] IETF RFC 2182. Selection and Operation of Secondary DNS Servers. July 1997. http://www.dns.net/dnsrd/rfc/rfc2182.html#4.Unreachableservers

[9] McCullagh, Declan. How, Why Microsoft Went Down. 25 January 2001. http://www.wired.com/news/technology/0,1282,41412,00.html

[10] Seifried, Kurt. DNS Server Infrastructure. 30 January 2001. http://securityportal.com/articles/dns20010130.html

[11] Weisman, Robyn. DoS Attacks: Internet Plague Without a Cure? 15 February 2001. http://www.newsfactor.com/perl/story/7050.html