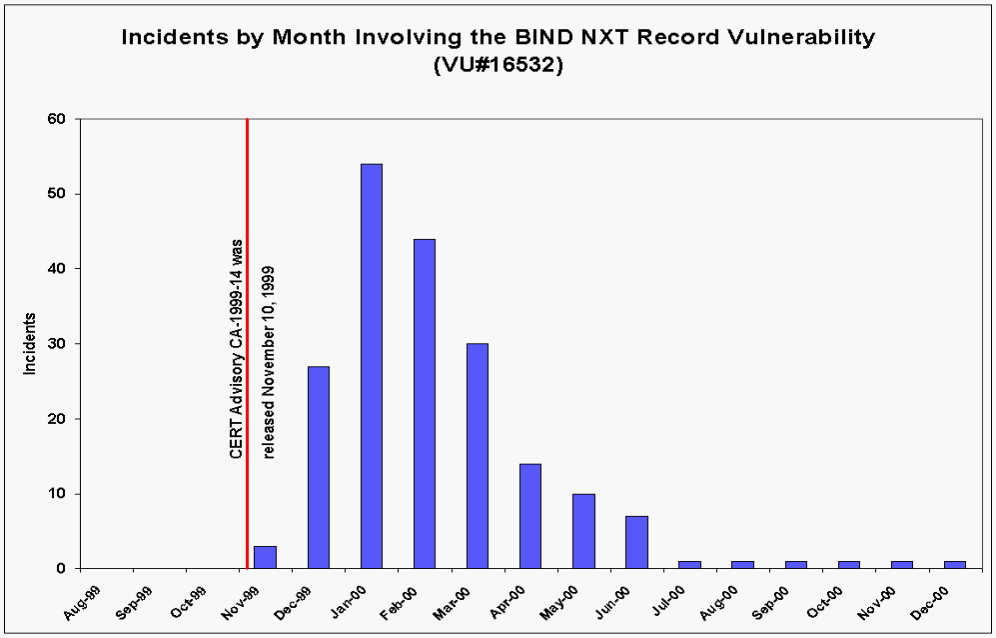
Global Information Assurance Certification Paper

By: I.E. (Jon) Naumann
GSEC Practical Assignment Version 1.2b

DNS Attacks: An Example of Due Diligence

"With the recent publicity over the Domain Name Service (DNS) attacks, it's become painfully obvious just how vulnerable the Internet's DNS infrastructure is." This was said in a 1997 article in the Unix Insider, written by Matt Larsen and Cricket Liu. It is now 2001, and the same statements are being made in response to the recent DNS attacks against Microsoft Corp.

Why? The simple answer is that new vulnerabilities are continuously being discovered. Does this mean that the solution to the problem is to apply the latest patches and continue on our merry Internet ways? In the light of statistics from Carnegie Mellon's CERT, this will not happen. As the graph shows, some diligent network managers will apply the patches, while the majority of others will not… At least not until they are attacked via the vulnerability.



CERT® Advisory CA-2001-02 Multiple Vulnerabilities in BIND Last revised: February 15, 2001

Why would you not apply the patches? An often heard answer is that system administrators do not have the time or inclination to stay on top of the myriad of vulnerabilities announced each year; that the need to get systems up and running and to provide services for their user base must come before security. Some claim that from reading the alerts of the vulnerabilities, that they require specialized knowledge and expert programming to exploit the vulnerabilities. Even though vulnerabilities have been announced for the latest version of BIND, there are as yet no known exploits for these noted vulnerabilities. So the impact of installing a new version of BIND, with the possibilities of disrupted service

within one's own organization, versus the ambiguous possibility of future exploitation, wins out.

DNS Vulnerabilities

To truly evaluate the threat, one needs to understand what are the consequences of DNS vulnerabilities. The first consequence would be DNS Spoofing. This is when a DNS server accepts and uses incorrect information from a host that has no authority giving that information. This erroneous information could then be used to change and reroute the numeric Internet addresses for Web access, electronic mail, and file transfers to arbitrary sites chosen by an intruder. An example here really brings this into focus: If an e-commerce site is spoofed via a DNS vulnerability, a company's customers could be redirected to an attacker's website to enter their credit card numbers!

The second consequence of a DNS vulnerability is the ability for an attacker to gain root access to the DNS server. This attack is usually perpetrated through the use of a "buffer overlow" vulnerability. This type of attack is formed when a program accepts more data from an outside source than it can store in the memory alloted for it. The extra data overflows into a portion of memory where instructions are stored, and can then be executed as though it were part of the original program. Once this has occurred, an attacker has a myriad of further attacks to perpetrate, including interception of data, insertion of false data into your system, insertion of distributed Denial of Service agents, and the use of your machine to attack other sites.

Which leads to one of the biggest consequences: civil liability. There are numerous laws against computer hacking. These laws include:

- Computer tampering – defined as intentional unauthorized access to a computer system.
- Aggravated computer tampering – defined as conduct that disrupts or interferes with vital services or operations or creates a strong probability of death or great bodily harm to one or more persons.
- Computer Fraud – defined as unauthorized access with intent to defraud or damage computer files.

Computer hackers can also be charged under federal law if the criminal activity stretches over state lines.

As reported in the Mar 17, 2000 edition of The Business Journal :

> Typical of the Internet reality, even if the hackers who wreaked this havoc could be found, chances are they would not be very good targets of civil suits. Although the actions of these hackers can cause significant economic loss in our emerging e-commerce economy, the perpetrators are unlikely to have the "deep pockets" necessary to make reparations for those damages.

> Accordingly, creative lawyers will search for others who may provide those "deep pockets." In the case of a smurf-like denial of service hack, the owners and operators of the networks who failed to protect against their systems' being used as a launching pad for such attacks, may become the prime targets.

What is Due Diligence?

The term due diligence is normally associated with the American securities laws. These laws impose very strict liabilities on the issuers of securities that are sold to the public and all those who assist in the process. Today, the term *Due Diligence* is applicable wherever a company provides services that affect the public.

BERG and DUFFY, LLP define Due diligence thusly:

> To begin, it is basically common sense coupled with a reasonable degree of skepticism. It does not mean you can not trust anyone or rely on experts. In fact, good due diligence does both to a very great degree. However, it does mean you can not rely on the report of a colleague or an expert if you know, or have reason to believe, it is not accurate or complete in any material respect. Nor is it possible to rely on a report, even if prepared in utter good faith, that is so hastily prepared no reasonable person could have made a satisfactory investigation of the matters reported on. Similarly, you can not rely on the report of a subordinate if it is clearly beyond his or her competence to perform. Thus, due diligence requires a considerable amount of seasoned good judgment and appropriate investigation of the material elements of the transaction.

How does Due Diligence fit into Network Security?

Taking the recent attacks on Microsoft as an example, the subscribers to Microsoft's Hot Mail service, Microsoft's TechNet service, and it's website were denied those services due to a Denial of Service attack on Microsoft's DNS server. The first attack centered upon the fact that of the Microsoft server's were co-located on the same network in the same physical location. This resulted in a misconfiguration on one server being replicated almost immediately to all servers. To repair the problem, all the DNS servers had to be taken off-line and repaired, thus leaving all of Microsoft's services without DNS while system administrators troubleshot & repaired the configuration errors. Once the servers were brought back on-line, attackers discovered that the new configurations were susceptible to a Denial of Service vulnerability, which was quickly exploited. Microsoft's CIO Rick Devenuti was quoted in the January 29, 2001 edition of InfoWorld magazine as saying "…we [Microsoft] did not apply sufficient self-defense techniques to our use of some third-party products at the front end parts of our core network infrastructure".

If the persons responsible for network security at Microsoft had applied *due diligence* to the security of their network, effects of these attacks could have been minimized.

How to close the existing DNS Vulnerabilities
The first step in closing these vulnerabilities is to determine which version you are currently running and on what machines. Then read CERT advisory **CA-2001-02** (www.cert.org/advisories/CA-2001-02.html), the CIAC advisory **J-063 DNS DoS Attacks** (ciac.llnl.gov/ciac/bulletins/j-063.shtml), and NAI's Covert Labs Security Advisory (www.pgp.com/research/covert/advisories/047.asp).

These documents describe how to obtain & install versions of DNS programs that are not susceptible to the currently known vulnerabilities. You'll also want to read these articles for advice on how to segregate your DNS servers. This is a topic that is often overlooked, but is important for many reasons. The first is to keep your internal network functioning in the event that your external DNS server is compromised. Another reason is to keep an attacker from using an external DNS server (that is usually not protected by a firewall) to attack your internal DNS server (which is usually inside your firewall).

Additional help for installing a secure DNS configuration can be found in Rob Thomas's **Secure BIND Template**, (www.cymru.com/~robt/Docs/Articles/secure-bind-template.html) as well as CERT's advisory CA96.21 for preventing TCP Syn flooding, (www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html) and also RFC2267 **Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address spoofing**.

Applying *due diligence* in your network
When applying network security to a network infrastructure, one needs to check all references possible. That includes reading trade journals (PC-World, SysAdmin Magazine, etc.), checking with security sites like SANS & CERT, as well as checking with other system administrators. A system administrator needs to use common sense and to look at the full impact of a given vulnerability and what liability his or her company is willing to bear should your system be attacked or used to attack the computers of another company.

As a system administrator, you can sign-up to receive periodic reports from Carnegie Mellon's CERT organization by going to www.cert.org/contact_cert/certmaillist.html. You can get similar information from Security Focus's (www.securityfocus.com) which has many mail lists which focus on specific types of vulnerabilities and operating systems. Max Vision's Whitehats.com also provides much needed information for the security conscious network administrator.

A system administrator should also use discretion if you choose to out-source network services such as DNS. If you choose a company without doing any

background research of its integrity (or choose a company even though it has a dubious track record) your company could still face liability in the event of an attack. It is wise to use your business library, the Better Business Bureau, and to conduct a search on the web when researching such companies.

Too often, system administrator's wait until they are attacked, or a major attack has been perpetrated on the internet before they begin to look at their own network. This is extremely dangerous for any company providing e-services. As a system administrator, you need to perform periodic scans of your networks & servers to test for known vulnerabilities. Tools such as Satan, Saint, and SARA are available on the web, and provide low cost tools to keep check on the integrity of your network. If you can afford the cost (or do not have the expertise "in house") you could hire a security company to perform a security assessment of your network. There are also companies which provide managed security services, although here again you'll want to research these companies before using their services.

Creating a schedule to check with manufacturers for patches is a good policy. Never assume that the latest release of an operating system is secure. Always check the vendor for patches before installing an OS. Some vendors offer software maintenance subscriptions, which could be used to automate this process.

Conclusion

Security is not only for security products like firewalls and encryption software. The great majority of vulnerabilities are a result of flaws in ordinary programs. Things like mail servers, spreadsheets, word processors, help programs, Web servers, and other such programs that are used everyday are the same programs that intruders use to gain unauthorized access to your systems.

Security products certainly help, but they are not a substitute for secure programs and procedures. Unless you behave like security really matters – and it does – then your networks won't be secure. Due diligence is required to check your network and examine all the vulnerabilities detected, even if you think that they are minor. It's those vulnerabilities that you may think are to insignificant to require your time to repair, that are the ones an attacker will exploit to gain unauthorized access to your network.

It is also very important to prepare an Incident Response Plan for the event that you are attacked. Who says what and when can sometimes be more damaging than the attack itself. Looking back, the quote of Rick Devenuti, Microsoft's CIO, could very well have caused his company problems by admitting that his company had failed to implement proper security procedures to protect their network. This type of public admittance could be used adversely if Microsoft were to be sued by their customers.

Here again, planning and research are of utmost importance. The need to respond to public inquiry in the aftermath of an attack must be weighed with the company's need for propriety. Lawyers can exploit the smallest mistake in disclosure just as an intruder can exploit the smallest vulnerability of your network.

Citations:

1. Larson, Matt & Liu Cricket. "Using BIND: Don't get spoofed again". UNIX Insider. Nov. 1997. URL: http://www.sunworld.com/sunworldonline/swol-11-1997/swol-11-bind_p.html (01 Mar 2001)
2. Olavsrud, Thor. "Security Flaws Found in Popular DNS Software". Internet news.com. January 19, 2001. URL: http://www.internetnews.com/wd-news/article/0,,10_573191,00.htm (01 Mar 2001)
3. Weiss, Todd R. "Microsoft admits defense against attacks was inadequate". Infoworld.com. URL: http://www.infoworld.com/articles/hn/xml/01/01/29/010129hnmsadmit.xml (2APR2001)
4. Duffy III, James P. "Some Thoughts on Due Diligence". BERG and DUFFY, LLP. December 15, 1995. URL: http://www.bergduffy.com/Personnel/95ddartl.htm (02 Apr 2001)
5. Turner, Glen. "J-063: Domain Name System (DNS) Denial of Service (DoS) Attacks". U.S. Department of Energy. Sept. 1, 1999. URL: http://ciac.llnl.gov/ciac/bulletins/j-063.shtml (02 Apr 2001)
6. Lanza, Jeffery P. "CERT Advisory CA-2001-02 Multiple Vulnerabilities in BIND". CERT/CC. Jan 29, 2001. URL: http://www.cert.org/advisories/CA-2001-02.htm (02 Apr 2001)
7. Thomas, Rob. Secure BIND Template Version 2.1". 03 FEB 2001 URL: http://www.cymru.com/~robt/Docs/Articles/secure-bind-template.html (02 Apr 2001)
8. Osborne, Anthony and McDonald, John "Vulnerabilities in BIND 4 and 8". PGP Security. Jan 29, 2001. URL: http://www.pgp.com/research/covert/advisories/047.asp (02 Apr 2001)
9. Rojas, Jose. "Recent hacker attacks might lead to novel civil claims". Business Journal, The. Mar 17, 2000. URL: http://southflorida.bcentral.com/southflorida/stories/2000/03/20/focus3.html (02 Apr 2001)
10. Kyl, Jon (Senator)."National Information Infrastructure Protection Act of 1996". THOMAS -- U.S. Congress on the Internet.1996.URL: http://thomas.loc.gov/cgi-bin/query/C?c104:./temp/~c104TX0jvA (02 Apr 2001)