GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

DNS Spoofing (Malicious Cache Poisoning)

Doug Sax

Introduction.

DNS Spoofing is best described as a DNS name server making use of false information received from a host that is not the authority for that information. It's a significant security threat to those organizations that have not taken steps to protect against it. DNS Spoofing can allow attackers to access a site's e-mail, it can cause users to be redirected to the wrong web sites even be the opening move in a denial of service attack.

Scope.

This paper will attempt to:

- Describe two types of DNS Spoofing attacks.
- Describe the possible results of malicious spoofing.
- List the recommended fixes for UNIX and Microsoft DNS.
- List informational links for more specific information.

Method.

Scenario: Your company, TAMJTek Inc., is racing to finish the development of the ultimate thing-a-ma-jig before your venture capital runs out. You start advertising the pending announcement of your breakthrough in thing-a-ma-jig technology on your Internet web site. You get a call from one of the partners in the venture capital firm. She wants to know why she ends up on www.hackncrack.net when she tries to go to www.tamjtek.com. You try connecting to your web site and, sure enough, you end up on www.hackncrack.net. You test a few other sites and everything seems fine except, you find that your strongest competitor has announced a thing-a-ma-jig breakthrough. Their web site shows a picture of their thing-a-ma-jig and it looks remarkably similar to yours with virtually identical specs. Coincidence? Maybe not.

Early this year an application developer, while testing software, discovered that a substantial number of on-line companies were vulnerable to DNS Spoofing. This vulnerability makes the TAMJTek Inc. scenario possible. One well-known example of DNS Spoofing occurred in 1997 when Eugene Kashpureff redirected users attempting to connect to the InterNIC domain registry to his own web site, AlterNIC. Mr. Kashpureff used the method of adding false record data in the answer to a query. Most recently, DNS Spoofing and domain hijacking was accomplished using only e-mail and a fax.

Example 1: Assume the following two domains, hackncrack.net and tamjtek.com with the following configuration:

Hackncrack.net (10.0.0.0)	Tamjtek.com (11.0.0.0)
ns1.hackncrack.net (10.0.0.5)	ns1.tamjtek.com (11.0.0.5)
www.hackncrack.net (10.0.0.6)	www.tamjtek.com (11.0.0.6)

© SANS Institute 2000 - 2002, Author retains full rights.

The attacker has modified the Hackncrack name server to respond to a recursive query for Hackncrack DNS records with a false authoritative record, mapping www.tamjtek.com to the 10.0.0.6 IP address. The attacker then directs a query to the TAMJTek name server asking for DNS records about the attackers own site. The TAMJTek name server resolves the query by going to the Hackncrack name server. Since the TAMJTek name server is not protected against DNS Spoofing, it accepts and caches the false record that's included in the answer. Whenever a query is made for the TAMJTek web site, the record for the Hackncrack web site will be returned and everyone will be redirected to www.hackncrack.net. The attacker at Hackncrack can also spoof an MX record to direct TAMJTek e-mail to his mail server. A false MX record can go undetected for a significant amount of time if the attacker is knowledgeable.

Example 2: By predicting the Query ID number, an attacker can carry out another adaptation of DNS Spoofing by impersonating a name server. The DNS protocol uses the UDP protocol to communicate. Given the connectionless nature of UDP, DNS is designed to establish orderly communications between hosts. This is accomplished by identifying datagrams with a Query ID number. The host that initiates the query assigns this number. In older versions of BIND, it's incremented sequentially for each new query. With this example you'll see how the attacker tricks the users at TAMJTek.com into thinking that they are going to www.AnyBank.com when, actually, they are connecting to www.Hackncrack.net. The attacker at Hackncrack.net queries TAMJTek.com for information on the attackers own domain. The TAMJTek name server resolves the query against Hackncrack.net. The attackers name server returns the correct information about itself to TAMJTek.com and the victim's name server relays it to the attacker's host that initiated the query. To mount this attack, the attacker has to, first, learn what the query ID number is. Sniffing the data during the query can achieve this. Once the ID number is in hand, the attacker crafts a DNS answer datagram with the false information: www.AnyBank.com = 10.0.0.6 and configures it to look as if its source were ns.AnyBank.com. The attacker initiates a query to TAMJTak.com asking for information about AnyBank.com and inserts the modified datagram on the wire as the answer. Once again, the unsecured TAMJTek.com name server accepts and caches the data. When the user at TAMJTek tries to connect to www.AnyBank.com, they get redirected to a specific web page on the Hackncrack web server that looks exactly like the AnyBank.com account information page. At this point, the attacker can collect user account and PIN numbers at will.

Example 3: This example does not describe a DNS Spoofing attack in the strictest technical sense of the term but, the end results are the same and it could be said that the this style of attack has the potential to "poison" the cache of every name server on the internet. Network Solutions Inc. was the first and still is one of the primary domain name registrars. During the registration process, NSI offers three methods of authorization and authentication to protect the registrant's records from unauthorized updates. These methods are collectively referred to by NSI as "Guardian". The contact person that is listed on the domain name record is also known as a Guardian. These methods are:

1. Mail-From (Least Secure): The contact submits an e-mail address from which all record administration will originate. When a record change is submitted to NSI via e-mail, the source e-mail address is compared to the e-mail address submitted during the original domain setup.
2. Crypt-Password (Somewhat secure): During the initial setup, the contact chooses a password. That password is encrypted and stored in NSI's database. When the administrator submits a record change, the plain text version of the password is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

included. NSI encrypts the plain text password accompanying the change request and compares it to the original.
3. PGP (Most secure): NSI supports PGP encrypted messages if they originate from a UNIX platform. No other platforms are supported at this time.

Well known names such as Nike, Net Media, Web Networks, Exodus and the World Wide Web Consortium have been affected by the circumvention of the DNS record update authentication process. During one incident, the ownership of Internet.com and 1300 other domains was transferred away from Net Media when NSI received a fax consisting of forged documents. It took several days for the legal owner to regain control of these domains. Imagine the havoc someone could wreak just being able to read the corporate e-mail that was redirected during the confusion. Obviously, the more secure the authentication process, the more secure the domain records.

Securing DNS

An in depth discussion on this topic is outside the scope of this paper but a list of relevant links to resources is included at the end. The following list has been included as a general reference for what could be done to help secure your particular DNS configuration:

1. Use the newest version available generally diminishes the possibility of attack.
2. Restrict or Authenticate Zone Transfers.
3. Restrict Dynamic Updates.
4. Turn off Recursion and Glue Fetching or Restrict Queries.
5. Install a Split DNS Configuration
6. Be informed. Follow the pertinent DNS Newsgroups (some links provided).
7. Use the most secure option possible to update your domain records.

Conclusion

In an Info-Sec.com web site article, http://www.info-sec.com/internet/99/internet_011199a_j.shtml (11/13/2000), asserts that one in three organizations with an Internet presence is vulnerable to DNS Spoofing. This type of attack can cause your e-mail to be redirected as well as your users and customers to be redirected when attempting to connect to your web site and can negatively effect consumer confidence in your company. The simple act of increasing the level of security that you use to authenticate record updates with your domain registrar can greatly increase your DNS security. In an 11 January 2000 by Chris Oakes article on Wired.com http://www.wired.com/news/business/0,1367,36797,00.html a Network Solutions spokesperson Brian O'Shaughnessy is quoted as saying "… the tools have – since 1996 – been available to our customers to protect themselves,". In the same article Mr O'Shaughnessy indicates that "… the onus is on the registrant to see that his domain is secure.".

Points to consider:

1. Your corporate e-mail could be read, compromising trade secrets and causing your company to loose it's competitive edge.
2. Corporate users and customers may be redirected to web sites other than your own, causing loss of customer confidence and, perhaps law suites (if directed to objectionable sites).
3. Users and customers could be redirected to an attacker's web site for the purpose of infecting their workstations with a virus.
4. Web site redirection could result in having your customers account information recorded on an attacker's web site.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

These are only a few possible exploits involving the DNS Spoofing vulnerability and there are, probably, many more waiting to be discovered. Discovery and implementation is limited only by the active imagination of the attacker.

Resources.

BIND Mailing Lists, Newsgroups and other resources.
http://www.isc.org/products/BIND/
The SANS Institute Newsletter subscription page.
http://www.sans.org/newlook/digests/SAC.htm
bind-users@isc.org Join by sending an e-mail to bind-users-request@isc.org
CERT mailing list. Join by sending an e-mail to cert-advisory-request@cert.org

MS DNS Server Resources.
http://www.microsoft.com/downloads/search.asp?
MS Product Security Notification Service. Subscribe by sending e-mail to
Microsoft_security-subscribe-request@announce.microsoft.com
The SANS Institute Newsletter subscription page.
http://www.sans.org/newlook/digests/SAC.htm
CERT mailing list. Join by sending an e-mail to cert-advisory-request@cert.org

Sources.

1. Network Solutions Inc. "Frequently Asked Questions about Authentication (Guardian)". URL: http://www.networksolutions.com/help/guardian.jhtml (11/13/2000)

2. Men & Mice. "DNS Security". URL: http://www.menandmice.com/infobase/mennmys/vefsidur.nsf/index/6 (11/13/2000)

3. Men & Mice. "DNS Glossary". URL: http://dnsinfo.menandmice.com/glossary/ (11/13/2000)

4. Lui, Cricket. "Securing an Internet Name Server" . URL: http://www.acmebw.com/papers/securing.pdf (11/13/2000)

5. Acme Byte & Wire LLC. "Papers and Presentations" web page. URL: http://www.acmebw.com/paper.htm (11/13/2000)

6. Microsoft Inc. "How to Prevent DNS Cache Pollution". 4 November 1999. URL: http://support.microsoft.com/support/kb/articles/Q241/3/52.ASP (11/13/2000)

7. Microsoft Inc. "Microsoft DNS Registry Parameters, Part 1 of 3". 20 November 1999. URL: http://support.microsoft.com/support/kb/articles/Q198/4/09.ASP (11/13/2000)

8. Lawson, Nate and Garris, John, PC Magazine. "Spoofing the DNS Server". 11 May 1999.URL: http://www.zdnet.com/devhead/stories/articles/0,4413,2257410,00.html (11/13/2000)

9. Erdfelt, Johannes. "Everything you ever wanted to know about DNS Spoofing" 25 July 1997. URL: http://www.the-project.org/admins/0797/msg00070.html (11/13/2000)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. Underground Security Systems Research. “DNS Abuse”. URL: http://www.ussrback.com/docs/papers/protocols/mi004en.htm (11/13/2000)

11. Lane, Diana B. “DNS Spoofing and Windows NT DNS”. 4 April 1999. URL: http://www.securiteam.com/windowsntfocus/DNS_Spoofing_and_Windows_NT_DNS.html (11/13/2000)

12. Bicknell, Craig. “NSI’s Webjacking Epidemic”. 8 June 2000. URL: http://www.wired.com/news/business/0,1367,36797,00.html (11/13/2000)

13. Oakes, Chris. “Domains Hijacked from NSI”. 11 January 2000. URL: http://www.wired.com/news/business/0,1367,36797,00.html (11/13/2000)

14. Wallock, Todd. Untitled. 28 July 1997. URL: http://www.nwfusion.com/archive/1997/97-07-28____.html (11/13/2000)

15. Wired News Report. “Webjackers Do It to Nike”. 21 June 2000. URL: http://www.wired.com/news/business/0,1367,37146,00.html (11/13/2000)

16. Seifried, Kurt. “DSN spoofing/registering/etc”, BUGTRAQ Archive Message ID 001901bf53c9$b42a82c0$1e00010a@edmontonint.seifried.org. 31 December 1999. URL: http://www.securityfocus.com (11/13/2000)

17. www.Info-Sec.com. “A Serious Threat to the Internet Community”. 11 January 1999. URL: http://www.info-sec.com/internet/99/internet_011199a_j.shtml (11/13/2000)

18. Albitz, Paul, Larson, Matt and Lui, Cricket. “DNS on Windows NT”. October 1998. O’Reilly & Associates, Inc.

19. Albitz, Paul and Lui, Cricket. “DNS and BIND”. January 1997. O’Reilly & Associates, Inc.

© SANS Institute 2000 - 2002, Author retains full rights.