Global Information Assurance Certification Paper

Naptha, the latest Denial of Service Vulnerability

Ann Compton

December 3, 2000

In February of this year, all of us were reminded of the havoc that a Denial of Service (DoS) attack can have on any system. For two days we heard of well-known sites such as eBay and Yahoo falling victim to a DoS attack. This practical will document current information available on this latest DoS vulnerability, Naptha, provide a general overview of the elements of a DoS attack and outline its effects on Windows operating systems.

When using the DoS vulnerability an attacker is attempting to negate service to users of that service. The CERT Coordination Center gives the following examples of this type of attack.

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person.[1]

In the same internet article CERT outlines threes ways of accomplishing these types of attack. The first is to consume "scarce, limited, or non-renewable resources".[2] A perfect example of this type of attack is the SYN attack in which an attacker sends packets to a server, often with fake addresses. The attacker sends a SYN message to the server. The server replies with the SYN-ACK message to the client. However the client does not respond with an ACK message. The server will then use up valuable resources trying to service the connections that are not real. Another type of attack can come within the network as described in our text wherein an intruder will connect one machine with the echo service to another machine with the chargen service on another.[3] The entire bandwidth between the two machines can be used up.

Secondly, an attacker may destroy or alter configuration. This attack of course can render a system unstable or unusable, thus stopping any type of service. Finally, if an intruder is able to gain physical access, then destruction can be done to components or machinery. Good physical security should be a part of any security policy as a preventive for this issue.

To make the issue even more complicated, Denial of Service tools are now available which allow one or more targets to be attacked at once (known as Distributed Denial of Service tools). CERT in Advisory CA-1999-17 describes one such tool called TFN2K. CERT notes some features of the tool are generating traffic that is both hard to recognize or to filter; the ability to execute remote commands; to hide the source of the traffic is hidden, and to use multiple transport protocols including UPP and TCP.[4] What makes this scenario even more interesting is the fact that the intruder will compromise a

machine and then issue commands to that machine to control other machines which then initiate the attacks.

In the published results of the Distributed-Systems Intruder Tools Workshop this model is outlined as follows:

"The 'intruder' controls a small number of 'masters', which in turn control a large number of 'daemons'. These daemons can be used to launch packet flooding or other attacks against 'victims' targeted by the intruder."[5]

The paper further indicated that in these type of attacks in 1999, daemons were distributed to several hundred sites. One can immediately see the impact of multiple attacks on the victim, causing disruption in service. It now appears that this can be done with very little resource usage from the attacker as will be outlined below.

On November 30, Bindview's RAZOR team identified a new security vulnerability as Naptha.[6] Bindview states that Naptha could affect seven major operating systems to include Microsoft, Novell, Solaris, and Linux. The TCP protocol is exploited to cause slow downs or disruption of services.

CERT notes that this attack is similar to the "syn" attack mentioned earlier. Whereas in the syn flood attack the focus was on the state "SYN RECVD", Naptha expands this to include other states such as "ESTABLISHED" and "FIN WAIT-1". CERT maintains that "Naptha" and similar attacks are even more hazardous for the following reasons:

- They can be done "asymmetrically" -- that is, the attacker can consume vast amounts of a victim's limited resource without a commensurate resource expenditure.
- In combination with other vulnerabilities or weaknesses, they can be done anonymously, and
- They can be included in distributed denial-of-service tools.[7]

Microsoft has identified this as a vulnerability in NT 4.0, 95, 98, 98 Second Edition and Windows ME. Windows 2000 is not affected. Microsoft notes that a flaw exists in the implementation of the NetBIOS over TCP/IP (NBT) protocol. They define NBT "as the protocol standard for how NetBIOS services are provided on a TCP/IP network".[8] In the affected operating system the implementation of the protocol, not the protocol itself appears to be the issue. Microsoft indicates that the problem occurs with incorrect handling of invalid data packets. This vulnerability can only be exploited if TCP Port 139 is open on the target machine.

There is a patch available for Windows NT 4.0. This patch has been tested with Service Pack 6a and repairs the error in the NBT implementation. Microsoft has provided no patch for Windows 95, 98, 98 Second Edition, or Windows ME. Only computers using File and Print Services are vulnerable. Microsoft recommends that machines should not enable File and Print Services with Dial-Up Networking. The File and Printer Sharing check box should be clear under the Properties, Bindings tab. This will only affect Dial-

UP Networking not local file sharing.

If a user must share files and printers on the dial-up adapter, Microsoft recommends unbinding File and Print Services to TCP/IP and then installing the NetBEUI protocol. A third solution that can be implemented on Windows 98 Second Edition is to install Internet Connection Sharing (ICS). Microsoft states that this should only be installed on the computer that you use to connect to the Internet.

This latest vulnerability confirms again the need to be part of a network that informs managers and system administrators of the latest security issues affecting systems. It also points to the need to continually keep systems updated with the latest patches identified as solutions. Are these solutions 100%? No, of course not, but efforts must be made to make our systems as secure as possible. As noted in the report from the Distributed-Systems Intruder Tools Workshop, these new tools "demonstrate that the security of any site on the Internet depends, in part, on the security of all other sites on the Internet". In effect, we are all responsible for a secure computing environment.

[1] CERT® Coordination Center Software Engineering Institute. "Denial of Service Attacks." 12 February 1999. URL:http//www.cert.org/techtips/denial_of_service.html.
[2] Ibid.
[3] Northcutt, Stephen. "Information Assurance Foundations." 28 June 2000.
[4] CERT® Coordination Center Software Engineering Institute. "CERT® Advisory CA-1999-17 Denial of Service Tools." 3 March 2000. URL:http//www.cert.org/advisories/CA-1999-17.html.
[5] CERT® Coordination Center Software Engineering Institute. "Results of Distributed-Systems Intruder Tools Workshop.: 7 December 1999. URL://www.cert.org/reports/dsit-workshop.pdf.
[6] "BindView Uncovers Major "Naptha" Security Vulnerability in Multiple Operating Systems." 30 November 2000. URL:http//www.bindview.com/news.
[7] CERT® Coordination Center Software Engineering Institute. "CERT® Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks." 30 November 2000. URL://www.cert.org/advisories/CA-2000-21.html.
[8] Microsoft TechNet. "Microsoft Security Bulletin (MS00-091)." 30 November 2000. URL:http://www.microsoft.com/technet/security/bulletin/ms00-091.asp.
[9] Microsoft TechNet. "Microsoft Security Bulletin (MS00-091): Frequently Asked Questions." 29 November 2000. URL:http://www.microsoft.com/technet/security/bulletin/fq00-091.asp.
[10] Microsoft Product Support Services. "Disable File and Print Sharing for Additional Security" 20 October 2000. URL:http://www.support.microsoft.com/support/kb/articles/Q199/3/46.asp.

---

[1] CERT® Coordination Center Software Engineering Institute. "Denial of Service Attacks." 12 February 1999. URL:http//www.cert.org/techtips/denial_of_service.html.
[2] Ibid.
[3] Northcutt, Stephen. "Information Assurance Foundations." 28 June 2000.
[4] CERT® Coordination Center Software Engineering Institute. "CERT® Advisory CA-1999-17 Denial of Service Tools." 3 March 2000. URL:http//www.cert.org/advisories/CA-1999-17.html.
[5] CERT® Coordination Center Software Engineering Institute. "Results of Distributed-Systems Intruder Tools Workshop.: 7 December 1999. URL://www.cert.org/reports/dsit-workshop.pdf.
[6] "BindView Uncovers Major "Naptha" Security Vulnerability in Multiple Operating Systems." 30 November 2000. URL:http//www.bindview.com/news.
[7] CERT® Coordination Center Software Engineering Institute. "CERT® Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks." 30 November 2000. URL://www.cert.org/advisories/CA-2000-21.html.
[8] Microsoft TechNet. "Microsoft Security Bulletin (MS00-091)." 30 November 2000. URL:http://www.microsoft.com/technet/security/bulletin/ms00-091.asp.
[9] Microsoft TechNet. "Microsoft Security Bulletin (MS00-091): Frequently Asked Questions." 29 November 2000. URL:http://www.microsoft.com/technet/security/bulletin/fq00-091.asp.
[10] Microsoft Product Support Services. "Disable File and Print Sharing for Additional Security" 20 October 2000. URL:http://www.support.microsoft.com/support/kb/articles/Q199/3/46.asp.

Last Updated: May 30th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event