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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Internet File Sharing

Meredith Lynes
19 June, 2000
GIAC LevelOne - Internet Research Project

Napster and one of it's relatives Gnutella have spawned a great deal of interest in the last few months. This is almost certainly related to the media coverage of the RIAA lawsuit against Napster and America Online's (AOL) actions regarding Nullsoft's Gnutella. December of 1999 brought us RIAA's lawsuit claiming that Napster facilitates illegal distribution of copyrighted music. In March 2000 Nullsoft, makers of Winamp and Shoutcast, released a file sharing tool to the public. Within a day the project was closed down by AOL, Nullsoft's parent company, and a statement issued saying that Gnutella was an unauthorized freelance project, however not before the "slashdot effect" took it's toll and the software was downloaded and posted on numerous other sites. On Apr. 4, 2000, users of a popular cable modem service were sent an e-mail to inform them that using Napster would result in loss of their service. While Napster is designed only to share music files, Gnutella is an internet file searching/sharing program. This heralds a new era in the way users can find and retrieve data. It also presents network and system administrators with some new challenges, increased bandwidth requirements, unintentional file sharing, a new method of virus propagation, a new method of trojaning, and last, but not least, new exploits.

Gnutella is a search engine and file server rolled into one tidy little package. Simply enter a search term and any filename containing that word on the Gnutella network will be returned. Click on the filename and it will be downloaded to your computer. This could possibly be one of the most important developments in Internet technology since the search engine.

Gnutella is still somewhat crude. It could be difficult to figure out for the everyday Internet user, though well written tutorials and Gnutella network IP's are readily available. Gnutella is advertised as the answer to Napster's legal problems. Because there is no central server there is no company to sue for copyright violations.

Unlike popular search engines Gnutella is an anonymous method of search. It would be difficult to pinpoint where searches originate due to the fact that each client on the network acts as a node or a hub. While the IP of the requesting computer is shown during the downloading process, no logging is done within the Gnutella client.

Unlike Napster, which is client/server based, Gnutella and it's clones use a peer to peer model. In effect it creates it's own self perpetuating network. This makes Gnutella searches inefficient since every computer on the Gnutella network must be searched and at this time searches can not be narrowed down. This can become a bandwidth issue.

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

Another limitation is the inability to stop a search. While Gnutella claims to have incorporated bandwidth shaping limits into the software a novice user will most likely just use the default settings. However this same lack of central server is a major strength of Gnutella as there is no single point of failure. Users can not be knocked off line by a single computer outage. Because of its very nature Gnutella is almost unstoppable.

Another interesting feature of Gnutella is the "push request." This feature's entire function is to bypass firewalls. When Gnutella attempts to download a file it first tries a standard pull. If this is unsuccessful the requesting client then routes a request through the Gnutella network to the system behind the firewall . The firewalled system then pushes out the file.

Each Gnutella connection uses between 500 and 1000 BPS of bandwidth. In addition each Gnutella client typically broadcasts a ping every minute or so to discover all the other clients on the network. A 2000 client network will produce 4 billion icmp messages per minute. By it's very nature Gnutella may inadvertently produce a Denial of Service.

Many administrators have blocked the Gnutella's default port (6346) both ingoing and outgoing. Packet filtering is not an effective method of stopping Gnutella as the software is easily port configurable. The main Gnutella web site http://gnutella.wego.com very concisely details how to get around most network security measures, as well as offering a wide selection of gnutella clones. One of the recommended solutions is to use a port that is commonly open on a firewall i.e. ports 25, 110, 143.

"*Distributed nature of servant makes it pretty damned tough for college administrators to block access to the gnutella service. Ability to change the port you listen on makes it even harder for those college administrators to block access. Ability to define your own internal network with a single exit point to the rest of the internet makes it almost fucking impossible for college sysadmins to block the free uninhibited transfer of information*", states the documentation of version 0.2 of Gnutella. While this is outdated it does give some insight to the developers intent.

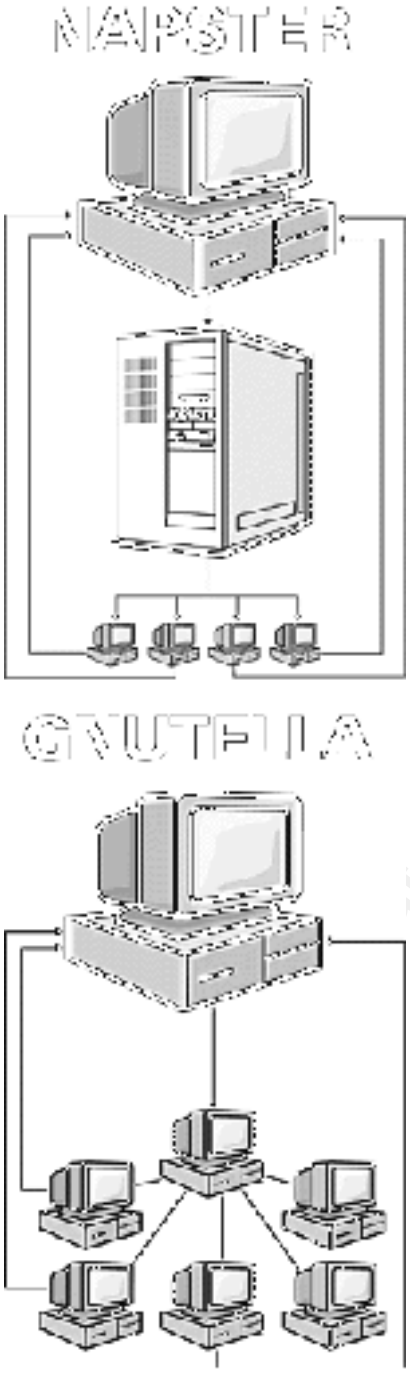
It has been speculated that the new generation of Gnutella clones will allow entire hard drive file searches rather then simple filename searches. This is certainly a powerful information searching technique.

Gnutella and Gnutella like clones are available for a range of OS's ranging from Microsoft versions to Mac and Linux. Bandwidth issues aside this type of search and sharing software can easily expose a firewalled network to data theft and compromise, particularly if users set up shared folders irresponsibly, thus effectively rendering the firewall useless.

There is no additional exposure to viruses using one of these programs other than those found in normal Internet web, ftp, irc usage.

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

In conclusion, Gnutella and it's clones may well bring about new power and freedom of information they should be regarded with a cautious eye in the business environment due to the difficulty of controlling their usage.



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

References:

1. Sullivan, Bob, "Software ignites porn, pirate worries", April 12, 2000
http://www.msnbc.com/news/393962.asp#BODY (19 June 2000)

2. Oakes, Chris, "Napster Not At Home With Cable", Apr. 7, 2000
http://www.wired.com/news/technology/0,1282,35523,00.html (19 June 2000)

3. Jones, Christopher, "Open-Source 'Napster' Shut Down", Mar. 15, 2000
http://www.wired.com/news/mp3/0,1285,34978,00.html, (19 June, 2000)

4. Manuka, "Gnutella & Firewalls", May 21, 2000
http://gnutella.wego.com, (19 June, 2000)

5. Barmann, Timothy C., "Software Sharing: Could it Change the Internet?", May 01 2000
http://www.wfaa.com/wfaa/articledisplay/0,1002,1_1_10493,00.html, (19 June, 2000)

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

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 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
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	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