Global Information Assurance Certification Paper

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.

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.

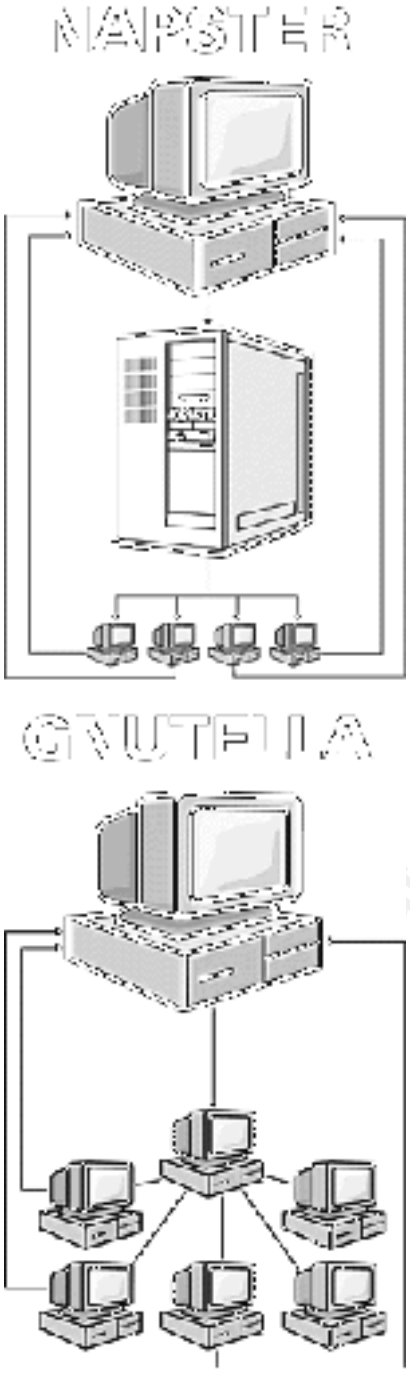
"*Distributed nature of servant makes it pretty damned tough for college administrators to block access to the gnutella service. Ability to change the port you listen on makes it even harder for those college administrators to block access. Ability to define your own internal network with a single exit 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.

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.



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)

Last Updated: October 18th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive