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 Relay Chat – Pros, Cons and Those Pesky Bots

James Etherton

24 April, 2001

Background

When we once had to rely upon traditional means of communication such as the telephone, fax, carrier pigeon or what have you; we can now communicate instantaneously thanks to the Internet. This ease of communication has become pervasive in our everyday lives. Ask a teenager in the United States if they can remember a time when they didn't have an Internet connection and they will be hard pressed to answer. The popularity of the Internet has vast implications in today's society, mainly that people are now more interconnected than ever before. This has both positive and negative implications.

In this paper, I intend to briefly discuss Internet Relay Chat (IRC) and cover some of the pros and cons of the application, along with some of the bots or interesting scripts available to anyone with a desire for knowledge and a UNIX shell account.

History of IRC

IRC, or Internet Relay Chat, began in 1988, when Jarkko Oikarinen, an employee at the University of Oulu, set about to develop a way to communicate based on existing Bulletin Board System (BBS technology). He hoped to develop a way to share discussions in USENET type forums as well as real-time discussions.[i] Jarkko distributed the IRC program and its use spread within Finland, but it was not until sometime after that IRC came into widespread use. This was due to the lack of connectivity outside of Finland. IRC use really took off in 1991, when, U.S. service members used it to communicate with loved ones back home.

Use of Internet relay chat today is tremendous. Researchers, students, parents and children are only a few of the types of people who communicate via IRC. As with any technology, there is also a darker side to the use of Internet relay chat as a means of communication. IRC servers have become a haven for hackers, social deviants, and others with malicious intent. This dark side will be covered briefly, later in this paper.

So, how does one connect to IRC? There are a myriad of clients used to connect to IRC servers. These include applications for UNIX (type), Windows and Mac operating systems. The most common default port for IRC servers is

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

6667. Any search engine will turn up thousands of sites to download the client. Beginner users should use a client such as mIRC which can be downloaded at www.mirc.org due to the ease of installation and configuration. Conversely, more advanced users are attracted to products such as BitchX or PIRCH for the scalability and multiple platform support built into the software.

There are literally thousands of servers available for users to connect to. Internet.org generally classifies the servers based on content or by numbers of users each server can accommodate.[ii] IRC servers therefore fall into one of six categories. These are:

1. The Big Four: These networks have the most servers available with global coverage. Efnet is oldest of the big four, founded in 1996. A look at Efnet.org shows that the network has servers from Norway to the Philippines. Undernet is also one of the largest realtime chat networks in the world, with approximately 45 servers connecting over 35 countries and serving more than 1,000,000 people weekly. Undernet, IRCnet and DALnet also have the same breadth of coverage as Efnet – its just that they were all formed later. These servers typically do not operate as for-profit business.

2. The medium networks: The medium networks consist of servers That host over 500 users.[iii] These IRC networks have the same standards of operation as the big four; offering high access speeds and continuous connectivity. However, the medium networks do not have the geographical representation of the larger networks.

3. The small networks: These networks have significantly fewer servers than the previous categories. They typically have 10-20 servers with less capacity to support users. The small networks are usually self-regulating with the server administrators making up the governing body of the network.

4. The forth category is based on subject content of the server. Some examples are kidsworld, Amiganet, and others. These servers typically have less capacity to serve customers as well as limited, regional geographical scope.

5. Regional Networks: These networks are established to service specific regions. These networks typically service clientele based on regional or cultural needs. Some examples are brasnet.org in Brazil and oz.org in Australia.

6. The last category according to www.irchelp.org is the major, non-networked server. These providers host servers such as chat.talkcity.com

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

and www.chatcircuit.com. These servers are intended to be for profit entities.

Pros of IRC

IRC creates an environment for instantaneous communication where users can trade ideas and information in real time. The help pages for mIRC v.5.8 states "mIRC attempts to provide a user-friendly interface for use with the Internet Relay Chat network. The IRC network is a virtual meeting place where people from all over the world can meet and talk."[iv] While this is very simplistic, it embodies what IRC is about – a place for people to gather and interact.

A practical application built into IRC is the ability for administrators to make chat rooms which are available only by invite. This creates a private space for conversations to take place. Therefore, a good corporate use for IRC would be as a means for isolated branch operations to communicate with headquarters and vice versa. It is a cost effective alternative to phone, fax and other traditional means of communication. All one needs is a PC, an Internet connection and the ability to download the IRC client.

Another interesting feature of IRC is the direct client to client (DCC) suite. These functions allow users to bypass the IRC server by establishing direct connections with one another. Within the functionality of the suite is the DCC send which allows one user to directly send another user a file, the DCC chat which allows two users to establish a private chat session via a peer-to-peer connection.[v] There are downsides to the DCC usage that will be discussed in the Cons of IRC section.

IRC networks are configured in a way to create redundancy and reliability. If a user connects to mclean.va.us.undernet.org and joins a room #vintagecars users in the same chat room can be connecting from any myriad of other servers. Because of the sheer number of servers available, a user can be virtually guaranteed of a connection at any given time.

This is advantageous to users who need consistent connectivity, but IRC servers will typically allow only a fixed number of connections from outside of its domain. Therefore in order to assure a connection, it is best for the user to find a server near them.

Cons of IRC

Because there is no over-arching authority to act as a watchdog governing IRC servers, anyone can establish a server and join an IRC network. While most

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

networks have rules of behavior, it is very difficult for the network administrators to police acts of misconduct. It is therefore very easy for anyone with a spare computer and LINUX to build an IRC server to use for mischievous purposes.

As mentioned earlier, IRC allows users to establish peer-to-peer connections. This is fine as long as the data exchanged is innocuous. However, there are increasing instances of users downloading virii, trojans and other malicious code from IRC chat rooms either due to ignorance or willful disregard for appropriate security measures. Users must understand the implications of accepting any files from unknown parties. This is particularly true in IRC chat rooms where users trade .jpg, .mpeg, .bmp, and other file types. It is imperative to always be certain of the validity of the file prior to accepting it.

New users who have not properly configured their IRC client to prompt them when someone tries to send a file are prime targets for malicious bots and social deviants.

Not to point any fingers, there are a lot of automated scripts running rampant on IRC – most notably on Undernet servers. Not to say that Undernet administrators are not working proactively to create an efficient environment, but there seems to be a lot of automated processes running in friendly chat rooms such as #hawaiichat. This may be because Undernet is configured to allow channel server bots and some people have configured these bots to conduct malicious activities.

Bots

Bots (short for robots) are special programs that are written to take advantage of certain IRC features. Bots can be used to either enhance or detract from the IRC experience. The original intent of bots was to enable a 24-hour presence and a remote method for maintaining control of IRC chat rooms.

A bot's purpose is to remain on the IRC channel at all times and provide services to members of that channel. Also, bots may provide services to the clients of a certain server, or to the users of an entire network (botnet).

Scripts are programs used by clients to extend their sets of features in ways that either provide new functions for channel/ user management, or provide malicious features to disrupt others' IRC experience.[vi]

Types of Bots

There are basically three types of bots: War bots, Channel bots, and Bar bots.[vii] War bots are written to be malicious and cause chaos and havoc in channels. They can be used to do things like flood users, kick or ban them, add user names to K-line (do not allow) lists, etc. The use of these bots evolved from

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

the first use as a way to play practical jokes on your friends. Today, war bots are notoriously nasty. The only good reason to use a war bot is if there is someone in your channel that is being disruptive, annoying or who is otherwise bothering you or members of your channel.

Second, there are channel bots. Channel bots are a bit mundane, but can be useful. They will perform simple tasks like OP, DEOP, KICK and BAN. These bots are used to maintain the user lists, and conduct routine maintenance of the channel. Channel bots should only be used with your good friends, as they can control the bot and have it give them channel operator authority and have it kick or ban you.

Lastly, there are bar bots. Bar bots can be used to conduct social activities. They can serve drinks, food, and play games. However, their actions can become annoying to channel members quickly.

Bots are both useful and dangerous. They can be used to conduct any number of actions. A very interesting aspect of the bot is that they can be used together to form networks of interactive bots. This is known as a botnet.

Botnets

Bots can be linked together to form a botnet. This gives the bot administrators exponentially more power over resources. Basically, the administrator can talk to other people on the other bots' party line, share users, channel information, and any other function if all bots have the same scripts installed.

While botnets can be used for non-malicious activities, they also enable sharing of all aspects of those bots on the network. This means that the network can be used as a method of amplifying malicious activities.

Summary

While IRC is useful for facilitating communication, it also provides a conduit into networks for malicious activity. Administrators must remain constantly aware of the types of activities conducted within their networks. IRC is particularly difficult to monitor because of the numerous clients obtainable for download along with the thousands of servers available to connect to.

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

REFERENCES:

[i] www.ircbeginner.com/ircinfo/history-jarkko.html
[ii] www.irchelp.org/irchelp/networks/servers/
[iii] www.webchat.org/sub-menu/sm-serverapp.htm
[iv] mIRC v 5.8 Help files
[v] www.braindead.net/pugetsound/dcc.asp
[vi] www.xcalibre.com
[vii] Ibid. www.xcalibre.com/

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

Last Updated: April 24th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 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 Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
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 Columbia, MD 2017	Columbia, MD	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 Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	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