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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Using Big Brother to Verify System Availability

Mark Trimmer
November 22, 2000

System availability is one of the foundation precepts for computer security. Availability is typically defined as a loss of use. This can either be due to Denial of Service attacks, network issues, or host problems. There are plenty of costly systems out there that can monitor a network for availability such as Tivoli and OpenView but there are also some that are generally free. One such product is called Big Brother.

Introduction to Big Brother

Big Brother (BB) is a fairly simple and yet robust system availability scanner. The program is written mostly in a shell script or Perl and can easily be customized to an individual's needs or preferences. BB is broken down into several easy to manage pieces:

- The Server: The BB Server consists of a Unix box that performs network scans of remote systems and collects the data. Perl scripts are then run to take the collected data and create a dynamic web page that will be displayed on the BB Display.
- The Client: The BB Client is a locally run program that collects system specific information and transmits it to the BB Server.
- The Display: The BB Display is a web server that displays the current status of the systems monitored. The BB Display also can run Perl scripts to sort through the collected data to extra availability percentages and history logs.
- The Pager: The BB Pager is a system that will perform the paging function for BB. When correctly configured, BB can initiate a call to a beeper and leave a descriptive error message.

Big Brother uses a typical client/server model in performing it's tasks. The BB Server is a computer that runs the BB daemon program called "bbd". This little program is designed to listen on port 1984 (of course) for incoming messages from BB Clients. The BB Server also performs remote availability checking by connecting to BB Client machines periodically to determine if certain services are still running.

The BB Client runs a program called bbrun that performs the local system checks on memory utilization, disk space availability, base system processes, and message log checking. The client then transmits that information in a fairly simple format to the BB Server which collects the information.

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

The BB Display is where the BB Server will place the files necessary for the web page interface. The display only needs to be a functional web server where you can add programs to the /cgi-bin. While the update process is often, the file sizes are fairly small so there is not a lot of overhead. One of the newer features of the BB Display is a system availability calculation that can help determine chronic problems.

Installing Big Brother

The best way to understand Big Brother is to configure it for yourself. The place to start is http://www.bb4.com. From this site you can find a wealth of information regarding Big Brother, including accessing the support mailing list. Make sure that you have the necessary equipment to run BB since the server only runs on Unix/Linux platforms and requires a C compiler and Perl to already be installed. A web server is required to perform the Display function and a modem will be required if the Pager function is to be used. Clients are available for Unix/Linux, Windows NT, Novell, and Macintosh OS. For the purpose of this paper it is assumed that the Server and client are both RedHat 7.0 systems with all the latest patches and fixes running an Apache web server.

From the Big Brother site download the latest code (version 1.5d2) to a temporary location. Verify the MD5 checksum listed on the BB web page by typing "md5sum –t <temporary_location>/bb-1.5d2.tar.gz". The code generated by the md5sum program should be **exactly** the same as the code listed on the web site. Once you have determined that this is the file you were expecting you can extract it by changing directory to the temporary location where you stored the downloaded file and then typing "tar –zxvf bb-1.5d2.tar.gz". This will extract two files, README.FIRST and bb15d3.tar. Read the file README.FIRST before going any further. This file contains installation instructions that will be reiterated in this paper but the information **will** change as different versions of Big Brother are produced.

After you have read the file and are comfortable with the steps outlined so far, let's extract the code. First, su to root to perform the next few steps. Change directory to where you want to install Big Brother. The typical locations are /opt or /usr/local, either will work. I prefer to use /usr/local since the default installation of RedHat does not create an /opt partition. Once in the installation directory type "tar –xvf <temporary_location>/bb15d3.tar". This extracts two directories, bb15d3 and bbvar. Next, to make life easier I always create a symbolic link to the bb<version> directory by typing "ln –s bb15d3 bb".

Now that the code is extracted we have to make some configuration changes to ensure BB runs properly on the your system. Change directory to the new bb symbolic link. In this directory you will find four README files. Be sure to read all of them very carefully for installation, configuration, and security-related information. Change directory again to the install directory. Type the following command to run the configuration script, "./bbconfig <OS Name>". In our example the <OS Name> is "redhat".

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

The first question you are asked is if you want to prevent BB from running as root. This is an important security issue, do **not** run BB as root. Take the default option of "y" by pressing Enter. The next question is asking what user will be running the BB program. I suggest that you do not take the default of "bb" but rather you create a new account with a non-meaningful userid to discourage hackers from brute force password hacking your system. I set this to a user named "qwerty" since this is easy for me to remember and to type. After this you are asked if you want to preserve the old style directory structure used by older versions of BB. Again, I do not suggest this for security reasons. Take the default answer of "no" by pressing Enter.

"Use FQDN (y/n): [y]" is the next question. This is asking you if you would like to use Fully Qualified Domain Names. Take the default answer of "yes". The next two questions revolve around two other functions of Big Brother, the Display server and the Pager server. Most people perform all these functions on the same system as the BB Server and this is what the Big Brother configuration script suggests as a default. I would suggest this until you are more familiar with BB; take the default answers to both questions. The next two questions are redundant if you took the default answers for the last two questions but we are asked again, "Is this host a BBDISPLAY host" and "Is this host a BBPAGER host". Again, take the default answer of "yes". Big Brother has an e-mail alert function that is used to notify the administrator of errors and loss of use. You are next asked to enter a default recipient for these messages. Typically you want this sent to the user who will be running the BB Server (i.e. qwerty) but you may want to specify another user based on your own specific needs, I entered "qwerty@localhost".

Next, we get into some of the default web settings. First we are asked what the default base URL is going to be. I have always accepted the default of "/bb" but you may choose something else if you choose to obscure your installation since system information will be available at this sight. Next, you are asked where the CGI directory is. This is different on most servers. Be sure you know exactly where this is before you answer or else you may put executable programs on your web site in plain view. On RedHat 7.0 the default Apache CGI directory is "/var/www/cgi-bin". You are now asked for the base URL for the CGI scripts, by default this is "/cgi-bin" on most web servers.

After BB is through setting some configurations based on your answers it is now ready to set some web permissions. You are first asked to enter the web server user id. While the default is "nobody" on most systems, on RedHat 7 the default is "apache". After hitting enter you will be asked for the group name. Again, on RedHat 7 the default group for the web server is "apache".

Now BB is ready for you to compile the program. On the screen are the instructions for doing this. Make sure you follow the directions carefully. Change directories to ../src and type "make". This is the compiling process and should be watched for any errors. When that is done type "make install". This will move the compiled programs to the appropriate locations for running. Now,

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

type "cd ../.." as this will put you in the /usr/local directory. We need to make sure that the directories and programs you just installed have the proper ownership. To do this type "chown –R qwerty bbvar bb15d3". Now, make a link for your web server to follow by typing "ln –s /usr/local/bb/www /var/www/html/bb". The hard part is done! You are now ready to configure your installation of Big Brother!

Configuring Big Brother

Configuring Big Brother couldn't be easier. There is basically only two files that will need manipulation. Other files may be modified depending on your needs but for this simple example we will only make basic changes. The first, and most important, file we need to modify is in the bb/etc directory. The file is called bb-hosts. I suggest that you make a backup copy of this file for quick reference if you need it by typing "cp bb-hosts bb-hosts.bak".

Edit the bb-hosts file with your favorite editor. The first thing you will see is that it looks vaguely familiar. This is done on purpose to make it easy for you to configure. It is setup like a /etc/hosts file where the first field is the IP address and the second field is the host name. Now this is where it starts to get a little different. Instead of everything after the "#" being a comment, this is where the real work starts getting done.

Every bb-hosts file needs to contain at least the following qualifiers, BBNET and BBDISPLAY. Without these two items your Big Brother will not work properly. The BBNET is the computer where you will acquire the information about the other hosts. The BBDISPLAY is the computer with the web server where you will display the information. In our case, we configured this machine to do both of these features. The BBPAGER is for the notification system. While we will not configure this here it is another important feature in Big Brother. The rest of the items in the bb-hosts file are services that each specific host has running that you wish to monitor. For instance, if you have an FTP server running on this machine place ftp in the same line as the entry and BB will connect to this service to verify it's availability.

The services listed here are referenced against the BBNET's /etc/services file. If the service name matches up with a known port in /etc/services then BB will connect to that port on the remote system to check for connectivity. Typical services to monitor would be "ftp, dns, ssh, telnet, and http". The only difficult one to figure out is "http". This service requires a unique setup since it can be configured to run on multiple ports based on the virtual web name. To get around this problem Big Brother initiates a connection to a web server in the same manner as a web browser. If the request in bb-hosts reads "http://192.168.0.1/ " then Big Brother will connect to that IP address on port 80 which is the default. If bb-hosts reads "http://www.somewhere.com/" then Big Brother will resolve that host name through DNS and connect to the appropriate port.

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

The second file to configure is even easier than that. It is etc/security and does not currently exist. This file will help secure your system by only allowing connections from the systems listed. If the file does not exist at all then by default all systems are allowed to connect to the BB server.

Again using your favorite editor edit the security file. There are two formats you can use in this file. The first, and most straightforward, is to add a single IP address on a line. This IP you added now can connect to the BB server. The second format is a group method of adding systems. By adding a line containing the IP subnet address followed by a "/" and then the netmask for that subnet you can add an entire network at once. An example of this would be "192.168.1.0/255.255.255.0". This means that every computer with an IP address between 192.168.1.0-255 can connect to the BB server.

Starting and Stopping Big Brother

Starting Big Brother is fairly easy. While logged on as your BB user ("qwerty") execute the command "runbb.sh" located in the root directory for BB. This command will start the BB daemon and you should be off and running! A file named BBOUT will be created in the same directory. This file contains system messages that BB may generate while processing.

The script runbb.sh has a couple of command line options that will make controlling Big Brother a little easier. These are the typical daemon commands of start, restart, and stop. By using "runbb.sh stop" you will halt the Big Brother service. By using "runbb.sh restart" the service will stop and start and re-read all the configuration files for any changes you may have made.

The only missing piece to runbb.sh is a status command. Unfortunately you will have to perform this manually. I generally use the following command although you may want to use something different "ps –ef | grep qwerty". This command will print out a process list for the entire system and then only display the processes that contain "qwerty" somewhere in the line. As long as you see a process labeled bbd and a couple others with bbrun then everything is probably working fine. Be sure to check the BBOUT file for anything unusual.

Within the first few minutes a new web page should be created at "http://<your configured host name/bb/". From here you can monitor system activity, history, and even send and acknowledge pages to and from the system administrators once you have configured the BBPAGER.

Future of Big Brother

Installing Big Brother isn't enough, however. There are additional packages out there that have been developed to increase the monitoring capability of Big Brother. Several packages allow for database availability monitoring which is becoming more and more critical in today's fast paced business. Other packages, like Multi-Router Traffic Grapher (MRTG) have been modified to be included in the Big Brother display. This allows for quick and easy access to historical graphs indicating bandwidth utilization. This can be an

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

invaluable tool if you are searching for a timeframe when you may have been compromised.

While this system does not compensate for the lack of an Intruder Detection System (IDS) it can become very helpful to a resourceful system administrator. In the future I am sure that further modifications will be added to increase the capabilities of Big Brother.

In a conversation with Sean McGuire, the original author of Big Brother, he and I discussed the possibility of adding Nmap and Tripwire as additional tests that Big Brother can monitor and notify on.
The basic idea is that Nmap can be used as a method to check for any new ports being opened on a remote system. This data can then be stored locally to the Big Brother server and then checked against on subsequent scans. Tripwire would become something entirely different. Tripwire is designed to perform regular full system scans of the host computer to detect changes to critical files. Typical system checks are time consuming and not realistic for a system like Big Brother. My idea is that a limited subset of system files can be checked more often to try and detect a system breach when a hacker has started attacking your system but before he can clean-up his tracks. Such a system would need to use obscurification to protect itself from the wiley hacker and then transmit logs to the Big Brother server for comparison.

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

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

References

Sittler, Paul M. "Big Brother Network Monitoring System". The Linux Journal. August 1997. URL: http://www2.linuxjournal.com/lj-issues/issue40/2225.html (October 31, 2000).

Mohr, James. "Big Brother Is Watching". Linux Magazine. January 2000. URL: http://www.linux-mag.com/cgi-bin/printer.pl?issue=2000-01&article=guru (October 31, 2000).

MacGuire, Sean & Croteau, Robert-André. "Big Brother is still watching". 1999. URL: http://www.bb4.com/bbsans99.pdf (October 31, 2000).

Caruso, Jeff. "More management on the cheap". NetworkWorldFusion. June 7, 1999. URL: http://www.nwfusion.com/news/1999/0607apps.html (October 31, 2000).

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