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

Demystifying Network Monitoring
A Guide to Hardening Fedora Core 1 and Installing Big Brother

© SANS Institute 2004, Author retains full rights.

David Neufeld

Submitted February 15th, 2004
GSEC Practical Assignment 1.4b
Option 1: Research on Topics in Information Security Abstract

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Abstract

The purpose of this paper is to outline how to use defence in-depth concepts to configure Network Monitoring using Big Brother (hereinafter referred to as BB) running on Red Hat Fedora Core 1 (hereinafter referred to as Fedora).

Specifically it describes how to install and harden Fedora, configure apache to password protect the BB website, install and customize the BB server and client, and extend the default installation of BB to include larrd and bbgen.

2. Introduction to Big Brother

BB is a robust client server network monitoring software package that uses a dynamic website to display the status of your network infrastructure in near real-time. When a problem is encountered, it notifies the persons responsible for maintenance of the problem device. By default, the BB Server tests a variety of network services on remote machines such as Connectivity, ftp, http, https, smtp, pop3, dns, telnet, imap, nntp, and ssh. The BB client reports statistics for hard drive utilization, CPU usage, messages/logs, and monitors to ensure that important processes/services are running. Other tests can also be easily added with the use of external scripts, a plethora of which can be found at www.deadcat.net. Alternatively users can write their own tests in almost any language which can then be added to the monitoring system.

One of the most compelling reasons to deploy BB over other commercial products is the "Better than Free" (BTF) license, under which it is shipped. The BB website (www.bb4.com) states that the commercial license is only needed when

> "Big Brother is helping you or someone else (in the case of outsourcing) make money"[1].

Even if a commercial license is needed for your organization it is very affordable, prices can be found at http://www.bb4.com/purchase.html.

---

1 Quest Software." Big Brother System and Network Monitor - License:". January 1, 2004. http://www.bb4.com/license.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Recommendations

3.1 Hardware

Since no hardware recommendations are listed in the BB documentation, use the recommendations from Red Hat as a guideline. The Fedora release notes outline the following minimum hardware specifications:-

> CPU:
> Recommended for text-mode: 200 MHz Pentium-class or better
> Recommended for graphical: 400 MHz Pentium II or better
> Hard Disk Space (NOTE: Additional space will be required for user data):
> Custom Installation (Minimal): 520MB
> Server: 870MB
> Personal Desktop: 1.9GB
> Workstation: 2.4GB
> Custom Installation (Everything): 5.3GB
> Memory:
> Minimum for text-mode: 64MB
> Minimum for graphical: 192MB
> Recommended for graphical: 256MB
> Note that the compatibility/availability of other hardware components (such as video and network cards) may be required for specific installation modes and/or post-installation usage[2].

* Although this document outlines a Fedora installation using text mode and the above minimum configuration ought to work, I have never deployed this solution on such a dated system. I have succesfully configured BB to monitor a 50+ server infastructure utilizing a single 450MHz Pentium II class machine running 256 MB of RAM and a 8 GB hard drive.

3.2 Infastructure

This paper assumes that your infastructure has an operational NTP and DNS Servers. The DNS server should already have records for the BB Server.

4. Preparing the BB Servers

4.1 Install Fedora

2 Fedora Project, "Hardware Requirements." Fedora Core 1 Release Notes. 2003. http://fedora.redhat.com/docs/release-notes/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1) The following files must be downloaded from the Fedora website, http://fedora.redhat.com/download/mirrors.html or one of its official mirrors:-

yarrow-i386-disc1.iso (md5sum: 76ef22495d186580e47efd8d7a65fe6b)
yarrow-i386-disc2.iso (md5sum: fd23fe32fafe7557f5d1fa1d31100580)
yarrow-i386-disc3.iso (md5sum: 6a26b34069639d0c31465d4079a8e1b2)

Once these files are downloaded, confirm the MD5 checksums, burn the downloaded iso files to CD and choose the boot method, this process is outlined at http://fedora.redhat.com/download/.

2) If installing Fedora on older hardware and it has been booted from the CD it is recommended to test the RAM by typing *memtest86* at the command prompt. Once the test has completed press esc and reboot.

3) Press enter to start the graphical installation mode.

4) Verify that the media has burned correctly (follow the instructions and test all three CDs).

5) Once the tests have been passed, follow the below table for installation options

Option	Action	Explanation
Welcome to Fedora Core	Press Next	
Language Selection	English (English)	Sets default language
Keyboard Configuration	U.S. English	Sets default Keyboard layout
Mouse Configuration	Generic 2 Button Mouse (PS/2) Uncheck “emulate 3 button mouse”	This driver works well with most KVM switches.
Monitor Configuration	Select Monitor type from the list provided	This sets the horizontal and vertical sync of your monitor.
Installation Type	Select Custom	Only install the software packages we need.
Disk Partitioning Setup	Manual Partitioning with Disk Druid see Appendix A	Separate RAID partitions where used for the web and BB locations.
Boot Loader Configuration	Leave defaults and check “Use a boot loader password” and strong password when prompted	Sets authentication prompt when a user ties to load kernel option during boot.
Network Configuration	Select Edit and uncheck “Use DHCP” and enter the IP address assigned to this machine then press OK. Type in the hostname and under Miscellaneous	The BB software will be using FQDN so we need to make sure we use an IP address and hostname that is in our

© SANS Institute 2004, Author retains full rights.

	Settings fill in the details that correspond to you network environment.	DNS.
Firewall Configuration	Make sure the Firewall is enabled and check to allow www and ssh connections to pass through. Under the other ports settings add 1984:tcp.	To limit the attack surface and deploy defence in-depth concepts.
Additional Language Support	* I removed English (USA) and changed the system default to English (Canada)	Choose any additional languages needed
Time Zone	Select your local time zone and check System Clock uses UTC	Sets default time zone
Set Root Password	Please use a password containing at a minimum 8 alpha-numeric and special characters.	A strong root password needs to be used.
Package Selection	See Appendix B	Only install the minimum packages required
Boot Disk	Insert a blank diskette into the floppy drive and select “Yes I would like to create a boot diskette”	This can be used to boot the system if problems arise.
Finalise Installation	The last screen prompts that the installation is complete and to press Reboot.	To start the new Fedora OS

After the first reboot you will have to logon under the root account. The first thing you should do is create a non privileged user account. To add an account and set the password use the *adduser* and *passwd* commands.

It is recommended to never logon directly as the root user. Instead it is advised to log on with a regular user account and *su* into root when needed, this will ensure a proper audit trail.

4.2 Updating the system

Proper defence in-depth techniques will include a plan to keep all systems current with security patches and bug fixes. A recent posting from the Malaysian CERT team MA-063.012004 supplies clear evidence why it is imperative for Administrators to keep systems patched.

> MyCERT had received report of mass web defacements of about 157 websites, involving the .gov, .net,.com, .edu and .org. About 98% of the web defacements involved Linux machines and the rest involved Windows 2000 machines.
> ……
> Based on MyCERT^Ys analysis and findings of previous incidents, majority of web defacements were due to vulnerable and unpatched services running in the server. Web defacements involving Linux machines are due to running older versions of Apache servers, PHP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

scripts and OpenSSL. Like the IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft Front Page Extension vulnerability and WEBDAV vulnerability.[3]

Yum is a new utility introduced in Fedora that can be scripted to automatically update rpm packages located in a private or public repository. Although setting up a local repository and update cycle is beyond the scope of this paper, more information can be found at:-
http://www.phy.duke.edu/~rgb/General/yum_article/yum_article/yum_article.html

If the yum daemon is turned on Fedora will automatically download and install patches. Even the up2date utility uses yum as a backend. For these reasons it is a good idea to become familiar with this powerful tool. The file /etc/yum.conf should be updated to include the option "gpgcheck=1" at the end of both the [base] and [updates-released] sections.

Example:
```
[base]
name=Fedora Core $releasever - $basearch - Base
baseurl=http://fedora.redhat.com/releases/fedora-core-$releasever
gpgcheck=1
```

* Although by default yum installs kernel packages instead of upgrading them I include the "installonlypkgs=kernel" in the main section to ensure success.

Note: It is not advisable to mix non Fedora/Red Hat repositories with other package repositories as this will likely result in compatibility problems. [4]

Now that the gpg check option is enabled the Fedora's gpg key's need to be imported.

```
# gpg --import /usr/share/rhn/RPM-GPG-KEY-fedora
# rpm --import /usr/share/rhn/RPM-GPG-KEY-fedora
```

Now begin the update process. When updating with *yum* the first thing that should always be checked is the yum package itself. [5]

---

3 MyCERT. "MA-063.012004:MyCERT Special Alert- Mass Web Defacements of Malaysian Websites", 19th January 2004, http://www.mycert.org.my/advisory/MA-063.012004.html

4 Fedora Linux. "Repository Mixing Problems", January 24, 2004. http://www.fedora.us/wiki/RepositoryMixingProblems

5 Brown, Robert. "Automating Nightly Updates". YUM: Yellowdog Updater, Modified. 17 December 2003. http://www.phy.duke.edu/~rgb/General/yum_article/yum_article/node21.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# yum update yum
Gathering header information file(s) from server(s)
Server: Fedora Core 1 - i386 - Base
Server: Fedora Core 1 - i386 - Released Updates
Finding updated packages
……

# yum update
Resolving dependencies
Dependencies resolved
I will do the following:
…
Is this ok [y/N]: y
```

The first command will get the header information for every installed package included in the repository and if an update for yum is available, will prompt for installation. The second command will check for updates in the repository and output a list of installed packages that need to be updated. Press y and enter to confirm all updates. If the rpm package is updated you will need to rebuild its database with "*rpm –rebuilddb*" as root.

One can also check if any installed packages are not supported in the Fedora yum repository, this can be done with the command "*yum list extras*". This should list the fedora@redhat.com gpg key as an unsupported package which one will need to update manually.

Finally reboot the system to load the newly installed kernel.

4.3 NTP configuration

The Network Time Protocol now needs to be installed and configured so all logs will have a correct time stamp. It is assumed you already have access to a time server, preferably on a secure internal machine. To install the ntpd package we will once again use *yum*.

```
# yum install ntp
```

Configure your ntp settings by editing the /etc/ntp.conf file with the names of your time server and any needed keys. Now start the service "*/etc/init.d/ntpd start*".

4.4 SSH

To configure the SSH daemon to only accept connections for protocol 2 and disallow root logon, the /etc/ssh/sshd_config file needs to be updated. (A sample accomplishing the above is included in Appendix C).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. Hardening Fedora and Apache

The machine will be configured to store and display information pertaining to all monitored servers. This information could help a malicious user map out your network, identify week services and compromise your systems. It is therefore vital to protect the confidentiality, integrity and availability of both this server and the information it contains. Defence in-depth principles teach users not to rely on one technology or device to protect information. One must now start to harden the machine by removing unused services and groups, reviewing the firewall settings, configuring TCPwrappers and Bastille.

5.1 Disabling Unnecessary daemons [6]

To reduce the attack surface that malicious users can exploit, it is highly recommended to disable any daemon/service that is not needed. Fortunately, Fedora provides the *chkconfig* utility which can be used to configure daemon start-up settings.

```
# chkconfig –list | grep on
….
# chkconfig –level 123456 daemons off
# chkconfig –level 3 httpd on
```

After disabling services that are not needed by this machine one should be left with the below list:-

```
# chkconfig --list | grep 3:on
syslog          0:off  1:off  2:on   3:on   4:on   5:on   6:off
rawdevices      0:off  1:off  2:off  3:on   4:on   5:on   6:off
network         0:off  1:off  2:on   3:on   4:on   5:on   6:off
random          0:off  1:off  2:on   3:on   4:on   5:on   6:off
iptables        0:off  1:off  2:on   3:on   4:on   5:on   6:off
irqbalance      0:off  1:off  2:off  3:on   4:on   5:on   6:off
microcode_ctl   0:off  1:off  2:on   3:on   4:on   5:on   6:off
smartd          0:off  1:off  2:on   3:on   4:on   5:on   6:off
autofs          0:off  1:off  2:off  3:on   4:on   5:on   6:off
sshd            0:off  1:off  2:on   3:on   4:on   5:on   6:off
sendmail        0:off  1:off  2:on   3:on   4:on   5:on   6:off
crond           0:off  1:off  2:on   3:on   4:on   5:on   6:off
httpd           0:off  1:off  2:off  3:on   4:off  5:off  6:off
ntpd            0:off  1:off  2:off  3:on   4:off  5:off  6:off
```

To stop/start the services just configured, one can switch between run-levels:-

[6] Linux Magazine. “Operating System Hardening” August 2003. http://www.linux-magazine.com/issue/33/Operating_System_Hardening.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# init 5
# init 3
```

To test which daemons are still accepting connections use the netstat command:

```
# netstat –anp | grep LISTEN
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp    0      0 0.0.0.0:80          0.0.0.0:*       LISTEN     3946/httpd
tcp    0      0 0.0.0.0:22          0.0.0.0:*       LISTEN     2968/sshd
tcp    0      0 127.0.0.1:25        0.0.0.0:*       LISTEN     12/sendmail: accept
tcp    0      0 0.0.0.0:443         0.0.0.0:*       LISTEN     3946/httpd
```

Port 443 will be disabled during configuration of apache but is already being protected by the Defence in-depth steps taken during installation of the firewall.

5.2 Securing Users, Groups

At this point it is advised to remove unnecessary users and groups.

```
# userdel non_essential_account
# groupdel non_essential_group
```

The current list of users and groups can be found in /etc/passwd and /etc/group. After removing all non-essential users and groups one should be left with the following:-

# cat /etc/group	# cat /etc/passwd
• root:x:0:root • bin:x:1:root,bin,daemon • daemon:x:2:root,bin,daemon • sys:x:3:root,bin • tty:x:5: • disk:x:6:root • mem:x:8: • kmem:x:9: • wheel:x:10:root • mail:x:12:mail • man:x:15: • nobody:x:99: • rpm:x:37: • floppy:x:19: • vcsa:x:69:	• root:x:0:0:root:/root:/bin/bash • bin:x:1:1:bin:/bin:/sbin/nologin • daemon:x:2:2:daemon:/sbin:/sbin/nologin • sync:x:5:0:sync:/sbin:/bin/sync • mail:x:8:12:mail:/var/spool/mail:/sbin/nologin • nobody:x:99:99:Nobody:/:/sbin/nologin • rpm:x:37:37::/var/lib/rpm:/sbin/nologin • vcsa:x:69:69:virtual console memory nscd:x:28:28:NSCD Daemon:/:/sbin/nologin • sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin • mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin • smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin • pcap:x:77:77::/var/arpwatch:/sbin/nologin • apache:x:48:48:Apache:/var/www:/sbin/nologin • webalizer:x:67:67:Webalizer:/var/www/html/usage:/sbin/nologin

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

• utmp:x:22: • slocate:x:21: • nscd:x:28: • sshd:x:74: • mailnull:x:47: • smmsp:x:51: • pcap:x:77: • apache:x:48: • webalizer:x:67: • ntp:x:38: • myaccount:x:500: • brother:x:501:	• ntp:x:38:38::/etc/ntp:/sbin/nologin • myaccount:x:500:500::/home/myaccount:/bin/bash • brother:x:501:501::/home/brother:/bin/bash

5.3 Firewall and TCPwrappers Configuration

Fedora has changed the default installation of the iptables firewall so that when it is enabled during installation it will be by default in a stateful firewall configuration[7]. Until the deep inspection firewall[8] is achievable by iptables the stateful inspection configuration is by far the most advantageous. Since the stateful inspection method allows iptables access to the kernel tables of open connections one can use this information to decide the fate of packages. This allows one the opportunity to deploy an adaptive firewall. Beyond the scope of this paper, but instructions can be found in the paper "Adaptive Firewalls with IPtables" by William Stearns.[9]

To view your iptables configuration as root run "*iptables –L*". To configure extra ports use the "*redhat-config-securitylevel-tui*" command (note that it doesn't display current settings), you can use the *iptables* command.

The second layer of network defence is the configuration of TCPwrappers. TCPwrappers[10] restricts network services monitored by the tcpd daemon based on rules set in /etc/hosts.allow and /etc/hosts.deny files. To find if a service has been compiled to run under tcpd (TCPwrappers) run the *strings* command:

```
#strings –f /path_to_daemon | grep hosts_access
/usr/sbin/sshd: hosts_access
```

---

7 Fedora Project. "Installation-Related Notes" Fedora Core 1 Release Notes. 2003.
http://fedora.redhat.com/docs/release-notes/

8 Cartwright, David. "Stateful vs. deep inspection firewalls" . Jan 8th 2004.
http://www.computerworld.com/securitytopics/security/story/0,10801,88871,00.html

9 Stearns, William, "Adaptive Firewalls with IPtables" http://www.sans.org/rr/special/adaptive_firewalls.php

10 Red Hat, "Chapter 15. TCP Wrappers Configuration Files". Red Hat Linux 9: Red Hat Linux Reference Guide.
http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-tcpwrappers-access.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If “host_access” is returned above then this service can be protected using TCPwrappers. The configuration file /etc/hosts.allow file should be edited to allow local network traffic access to ssh and the loop back adapter access to sendmail.

```
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
Sendmail: 127.0.0.1:ALLOW
sshd:   192.168.0.:ALLOW
```

Then edit the /etc/hosts.deny file.

```
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
ALL:ALL: spawn (echo Attempt from %h to %d at `date` | tee -a
/var/log/tcp.deny.log | mail youre-mail@domain)
```

The above configuration logs the IP address, daemon and date of unauthorized connection attempts to /var/log/tcp.deny.log and then e-mails this information to youre-mail@domain.

5.4 Installing Bastille

Bastille is an OS hardening script that performs extensive lockdown procedures based on user input.[11] Follow the below instructions to install this package:-

```
# cd /tmp
# wget http://www.bastille-linux.org/perl-Curses-1.06-219.i586.rpm
# wget http://easynews.dl.sourceforge.net/sourceforge/bastille-
linux/Bastille-2.1.1-1.0.i386.rpm
# rpm –Uhv perl-Curses-1.06-219.i586.rpm Bastille-2.1.1-1.0.i386.rpm
```

```
# bastille -c
```

Type “accept” to continue and choose a positive response to all questions asked except the following:-

Would you like to set the default umask
Would you like to disable SUID status for ping?
Would you like to disable the gcc compiler
Do you have a remote logging host
Do you want to stop sendmail from running in daemon mode
Would you like to deactivate the apache we server
Would you like to bind the web server to listen only to the locahost

11 Bauer, Mick. “Paranoid Penguin: Seven Top Security Tools” February 01, 2004. http://www.linuxjournal.com/article.php?sid=7235

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Would you like to disable cgi-scripts
Would you like to install TMPDIR/TMP scripts
Would you like to run the packet filtering script

* Note: Fedora is not yet officially supported by Bastille which detects the system as a Red Hat 8 installation. On all testing I have performed with the above configuration all security settings are updated correctly and system stability has not been affected.

Reboot to load the new settings.

Check the /etc/hosts.allow file as bastille has appended another deny rule onto it. This has enhanced the defence in-depth configuration two fold by supplying two locations where a deny rule is found and now a malicious user will not be able to append an allow rule to the hosts.allow file to gain access. Unfortunately since this file is checked before the hosts.deny file, unauthorized attempts will no longer be e-mailed to the administrator or logged. This can be rectified by altering the rule as seen below:-

```
ALL : ALL : spawn (echo Attempt from %h to %d at `date` | tee -a
/var/log/tcp.deny.log | mail -s "Port Denial noted" youre-mail@domain):
DENY
```

6.0 Apache Configuration

To configure the BB website and enable password protection the http.conf file needs to be edited. Please refer to Appendix D for an example http.conf file that accomplishes both the above requirements. Note: the sample in appendix D does not load modules needed for ssl support, as a result the ssl.conf configuration file located in /etc/httpd/conf.d needs to be renamed. -

```
# mv /etc/httpd/conf.d/ssl.conf  /etc/httpd/conf.d/ssl.bak
```

The directory structure for the cgi-bin and auth directories can be created with:-

```
# mkdir /www/cgi-bin
# mkdir /www/auth
# chmod 755 /www/cgi-bin /www/auth
```

The configuration file in Appendix D is set to password protect both the bb/cgi-bin and /bb using MD5 encryption. Notice the “Require user username1 username2” option within Appendix D, these usernames need to added the apache password file. This can be done using the htdigest command:-

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Example
/usr/bin/htdigest –c /location_to_new_password_file Realm Username
Adding password for Username in Realm
New password:
Re-type new password:

In the above example the htdigest command is set to clear the current password file with the –c flag and a new file is created in the location specified, the Realm needs to match what the "AuthName" directive is set to and finally the account name you specify is added to the new file.[12] When adding new accounts to the above file you will not need to use the –c option, but remember to update the httpd.conf "Require user" directive and restart httpd.

Although beyond the scope of this paper the mod_security module can be added to the apache configuration to dramatically increase security. This module acts as an intrusion detection system using snort rules to block malicious connection attempts to the website. More information and installation instructions can be found at http://www.modsecurity.org/

7. Installing Big Brother

This paper does not include instructions on the configuration of sending pages or SMS alerts via a modem. This is due to the security ramifications of attaching a modem to machines operating behind our organization's firewall. Instead send all after hours alerts to e-mail enabled cell phones. If either of these alert options are needed in your environment please refer to the "Big Brother Installation and Configuration Guide" in the reference section.

Before beginning see if you qualify for the BTF license by referring to documentation located at http://bb4.com/license.html..

7.1 Big Brother Server Installation [13]

First setup the directory structure where BB will be installed then download and un-tar the package.

mkdir –p /usr/local/opt/tarballs
cd /usr/local/op/tarballs
wget http://bb4.com/dnld/bb-1.9e.tar.gz
tar –xzvf bb-1.9e.tar.gz
tar -xvf BBSVR-bb1.9e-btf.tar

12 Apache HTTP Server Documentation Project. "Authentication, Authorization and Access Control". http://httpd.apache.org/docs-2.0/howto/auth.html

13 Cook Craig. "Big Brother Installation and Configuration Guide" 2002-10-11 http://www.deadcat.net/viewfile.php?fileid=462

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# mv bb1.9e-btf ../
# ln –s /usr/local/opt/bb1.9e-btf /usr/local/bb
```

The above addition of the symbolic link will make future upgrades easier to apply and set the BBHOME variable in most extension scripts to the correct location. To start installation of BB server, run the configuration script and compile the source:-

```
# cd /usr/local/bb      (Read all README files)
# cd install/           (Read all README files)
# ./bbconfig linux
Accept the license agreement and follow the below suggestion:
What will be the user ID for BB [bb]: brother
Use FQDN (y/n): [y]
What host will be the BBDISPLAY [machine.domain.name]:
What host will be the BBPAGER [machine.domain.name]:
Is this host a BBDISPLAY host (y/n): [y]
Is this host a BBPAGER host (y/n): [y]
Enter the default e-mail address to send notifications to:
[root@bb.networkwreck.com] your_email@address
Enter the base URL for BB [/bb]:
Enter CGI directory [/home/www/httpd/cgi-bin]: /www/cgi-bin
Enter the base URL of the CGI scripts [/cgi-bin]: /bb/cgi-bin
Enter web server user id [nobody]: apache
Enter group name [apache]: apache
```

Complete the installation by following the instructions at the end of the above script including the below modifications

```
# ln -s /usr/local/  /home/brother/bb
# chown brother.brother /usr/local/bb /home/brother/bb
# chown –R brother /usr/local/bbvar /usr/local/opt/bb1.9e-btf # su – brother
# su – brother
$ cd /usr/loca/bb/src
$ make
$ make install
```

7.2 Customization of BB Server

Before starting the BB Server it needs to be customized to suite the local environment. This can be done by editing the /usr/local/bb/etc/bbdef-server.sh and bbdef.sh files.

*On my servers I only needed to modify the bbdef-server.sh file, making the following changes:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
BBLOGSTATUS="DYNAMIC"
BBNETTHREADS=5
PURPLEDELAY="15"
RUNOPTS="CONVHTMLTAGS ENABLE_DISABLE DATAMSG LARRD"
```

Now add this machine's information to the /usr/local/bb/etc/bb-hosts file. The bb-hosts file is where all network tests for all monitored machines are set and is the template used to create the BB display website. For more information about this file read /usr/local/bb/install/README. The BBConfig extension will be used to configure this file and makes administration much easier. Installation steps are outlined shortly. For initial testing you can edit the file to reflect the below modifications

```
# THE BIG BROTHER HOSTS FILE
# THIS FILE SHOULD BE THE SAME ON ALL SYSTEMS RUNNING BIG BROTHER
# CHANGE THIS FILE TO REFLECT YOUR ENVIRONMENT!
0.0.0.0 FQDN_of_this_SERVER # BBDISPLAY BBNET BBPAGER ssh http:// FQDN_of_this_SERVER/bb
```

Since Bastille disabled the option of following symbolic links via the webserver, it is necessary to modify BB file permissions and the web content. This should be done as root.

```
# mv /usr/local/bb/www /www/html
# ln –s /www/html /usr/local/bb/www
# chown brother.root /usr/local/bb/www
```

7.3 Testing the BB Server Installation

Now test the installation and configuration for errors by running the bbchkcfg.sh, bbchkcmds.sh, bbchkhosts.sh and bbchkwarnrules.sh scripts located in /usr/local/bb/etc. Disregard the BBPAGER error produced by bbchkcfg.sh as you will not be using a modem. Start the BB server, *su* back to the BB user and navigate to BBHOME and start the server:-

```
# ./runbb.sh start
```

Check the BBOUT file located in the BBHOME directory for any errors and make sure the server is listening on port 1984.

```
#netstat –anp | grep LISTEN
tcp    0    0 0.0.0.0:1984        0.0.0.0:*        LISTEN    6145/bbd
tcp    0    0 192.168.0.2:80      0.0.0.0:*        LISTEN    -
tcp    0    0 0.0.0.0:22          0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.1:25        0.0.0.0:*        LISTEN    -
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.4 Installing and testing BB Client Software

The BB Client sends local test results to the BB Server to install the below instructions.

```
# cd /usr/local/opt/tarballs/
# tar -xvf BBCLT-bbc1.9e-btf.tar
# mv bbc1.9e-btf/ ../
# chown brother bbc1.9e-btf/
# ln -s /usr/local/opt/bbc1.9e-btf / /usr/local/bbc
# chown brother bbc
# cd /usr/local/bbc/install
#./bbconfig linux
```

Answer the client installation inquiries using the same answers from the Server Installation and finish the client install as follows:-

```
# chown -R brother /usr/local/opt/bbc1.9e-btf/
# cd ../src
# make
# make install
# cp /usr/local/bb/etc/bb-hosts /usr/local/bbc/etc
```

Since Bastille changed the default log files we need to inform BB to monitor them. This is done by adding extra MSGFILE options bbsys.local file located in /usr/local/bbc/etc.

```
Example:
MSGFILE="/var/log/kernel"
MSGFILE="/var/log/syslog"
```

To allow the BB client to monitor the log files and report when a problem is encountered the big brother user needs to be able to read them:-

```
#chown root.brother /var/log/kernel /var/log/messages /var/log/syslog
#chmod 640 /var/log/kernel /var/log/messages /var/log/syslog
```

Test the client installation with the bbchk scripts located in /usr/local/bbc/etc directory, once past start the client. If the installation completed successfully the client should start, again if you are having problems please check the BBOUT file.

At this time your server should be monitoring itself and if any errors are found e-mailing an alert to the address specified during installation. To view the BB website point a browser to the FQDN of this machine followed by /bb.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.5 Installation and Configuration of BBConfig

BBConfig is an addition to the BB server that automatically creates the bb-hosts file and other configuration files. To install the package follow these directions:

```
$cd /usr/local/opt/tarballs
$ wget
http://www.deadcat.net/download.php?fileid=222&filename=BBConfig-1_9.tar.gz&location=3
$ tar -xzvf BBConfig-1_9.tar.gz
$ mv BBConfig-1_9 ../
$ cd ../BBConfig-1_9    (Read BBConfig.README)
$ perl install --bbhome /usr/local/bb
$ /usr/local/bb/runbb/sh restart
```

Once BB has been restarted go to BBHOME/etc/ and notice the three files that have been installed bb-conifg.INFO, bb-disp.INFO, and bb-os.INFO.

The bb-os.INFO file creates an OS tag which is then used in the bb-config file to keep things organized and produce a count of each OS client type. Edit this to reflect the different OS's in your environment and then rename it to bb-os.

```
Example bb-os file:
<bbos Linux>
<bbos  HPUX>
<bbos Solaris>
<bbos Windows>
```

The bb-dist file is a template for the way the bb-hosts file and the BB website will be displayed. Valid directives for this file are page, group-compress, bbset and view. They are used to configure multiple web pages or views on you display server. The page option creates a subpage web for machines using the same bbset or view directive wile the group-compress separates a group of machines on the same webpage. This allows for creation of machine groupings that will be displayed on the BB website, which can range from OS, hardware, services, departments, location, etc.

* In my last installation we had to monitor 50 servers that where administered between 5 different departments. We created 5 different bbset tags, one for each department and multiple bbview tags. Which where then used in the bb-config file to create separate webpage's that contained only the servers each administrator was responsible for.

```
Example bb-disp file:-
group-compress Infrastructure Servers
<bbset inf>
```

© SANS Institute 2004, Author retains full rights.

```
page HR Department HR Department Servers
group-compress HR Servers
<bbset hr>

page R&D R&D Servers
group-compress R&D Servers
<bbset rd>

# Creates an additional page that contain all servers set to “bbview
# all” in the bb-config file without re-running tests.
page all All Servers
group-compress All Monitored Servers
<view all>
```

To complete the operation, configure the bb-config file. This file is used to populate the bb-hosts, security, bbwarnsetup.cfg and the bb tab files. It lists all monitored machines there services and any extension scripts they should run. Ensure every machine uses a bbset and bbos tag that were created in the above example. It is also recommended to create template settings for machines that need similar network tests.

```
Example bb-config file
objectclass:    bigbrother

# We want to make sure security is enables as this will populate the
# BBHOME/etc/security file with ip addresses that are allowed to connect
# to the bb server on port 1984
security:       on
warnsetup:      on
#----------------------------------------
# warnsetup.cfg info
#----------------------------------------
objectclass:    warnsetup
bbwarn:         TRUE
svcerrlist:     disk:100 cpu:200 procs:300 msgs:400 conn:500 http:600
dns:800 ERR:999
trapcodes:      disk:2 cpu:4 procs:6 msgs:8 conn:10 http:12 dns:14 dig:14
ftp:16 smtp:18 fping:20 imap:22 mq:24 mrtg:26 nntp:28 pop3:30 pop-3:30
ssh:32 swap:34 telnet:36 ERR:0
entoid:         .1.3.6.1.4.1.7058
snmptrap_pgm:   /usr/bin/snmptrap
snmptrap_type:  CMU
ignforall:
pagehelpcode:   911
ttyline:        /dev/cuaa0
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
prefix:         T9
suffix:
pagedelay:      15
pagelevels:     red purple
pagelevelsmail: yellow
pagerecovered:  FALSE
pagetype:       EVENT
pagemaster:     root@localhost
pageaddhtmlpath: TRUE
cfgdelim:       ;
briefrcpt:

#----------------------------------------
# Templates
#----------------------------------------
# Linux template to monitor ssh and make sure telnet is not running
# it will also report if ssh, syslog or ntp process stop
objectclass:  template
name:         linux
services:     !telnet ssh
procpanic:    ntp sshd syslogd

# Sample template for HPUX
objectclass:  template
name:         HPUX
services:       ssh cron !telnet

#----------------------------------------
# Hosts
#----------------------------------------
host:             bb.server.com
ip:               192.168.0.1
bbservices:    BBDISPLAY BBNET BBPAGER
template:      linux
bbset:         inf
bbview:        all
msg:           /var/log/syslog:: error
disk:          98:99
procpanic_add:   sendmail

host:             monitored server 1
ip:               192.168.0.2
bbset:            HR
bbview:           all
template          HPUX
procpanic:      sendmail
```

© SANS Institute 2004, Author retains full rights.

As seen before you will be able to complete the BB installation it is time to start planning and do some research.
* I would strongly recommend reading the BBConfig.README file which contains all the options that can be included in the above files.

Once these three files are populated with your environments settings you can generate BB configuration files by running /usr/local/bb/bin/bbconfigure and restarting the BB server.

To make life easier it is recommend to create symbolic links to the new configuration files from the server etc directory to the client directory.

```
# mv /usr/local/bbc/etc/bb-hosts /usr/local/bbc/etc/bb-hosts.bak &
# ln -s /usr/local/bb/etc/bb-hosts /usr/local/bbc/etc/bb-hosts
# ln –s /usr/local/bb/etc/bb-bbexttab /usr/local/bbc/etc/bb-bbexttab
# ln –s /usr/local/bb/etc/bb-cputab /usr/local/bbc/etc/bb-cputab
# ln –s /usr/local/bb/etc/bb-dftab /usr/local/bbc/etc/bb-dftab
# ln –s /usr/local/bb/etc/bb-msgstab /usr/local/bbc/etc/bb-msgstab
# ln –s /usr/local/bb/etc/bb-proctab /usr/local/bbc/etc/bb-proctab
```

Restart the client for these new settings to take effect.

7.6 Configuring Alert Rules

Alerts are sent to users or groups based on rules in the bbwarnrules.cfg file, which is located at /usr/local/bb/etc/. The format of the rules in bbwarnrules.cfg can be a bit confusing at first glance but are well documented in this file. Please read and understand these formats before continuing.

Fortunately BBConfig will create the bbwarsetup.cfg file which creates groups based on the bbset and view directives. Since all machines in the bb-config file will need a bbset tag set these groups are a great way to base notification rules. Furthermore, BBConfig populates the bbwarnsetup.cfg file with new machines as they are added so the bbwarnrules.cfg file should not need to be updated as often.

The below example rules will alert admin@somewhere.com for all servers in the hg-local group from 6:00am to 6:00pm Monday to Friday then alert cell#@provider.net Monday to Friday from 6:01pm to 5:59am and all day Saturday and Sunday.

```
##########################################
# Enter your rules here

hg-local;;*;;1-5;0600-1800; admin@somewhere.com
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

hg-local;;*;;1-5;1801-05:59; cell#@provider.net
hg-local;;*;;0 6;*; cell#@provider.net

It is also advised to set the below rules which will notify admin@somewhere.com when a machine is disabled or enabled using the maint.pl cgi-bin (described shortly) or when a there a alert for a machine that does not match any rules.

notify-admin;;pagehelp;;*;*; admin@somewhere.com
unmatched-*;;*;;*;*;admin@somewhere.com

These rules are the most important portion of the Monitoring System as they can provide information to the Administrator on how the entire network is running even when he/she is away from the office. This can often lead to resolving small unknown problems before they become service outages or compromises. Also if a service fails without previous warning BB will usually notify the Administrator before a problem is reported by users or customers greatly increasing availability.

7.7 Extending the Server Infrastructure

One of BB greatest strengths is the ease in which it can be extended to include custom tests and added functionality. To increase the functionality of the default BB installation it is advised to install at a minimum Larrd, Bbgen and a cgi Maintenance called maint.pl.

7.7.1 Larrd Installation

Larrd is a application that parses through the BB log files and uses rrdtool to generate trending graphs of selected tests. Both rrdtools and Larrd need to be installed as described below:-

```
# cd /usr/local/opt/tarball
#wget http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/pub/rrdtool-1.0.46.tar.gz
# wget "http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/pub/rrdtool-1.0.46.tar.gz.md5"
# md5sum --check rrdtool-1.0.46.tar.gz.md5
rrdtool-1.0.46.tar.gz: OK
# tar -xzvf rrdtool-1.0.46.tar.gz
# cd rrdtool-1.0.46 (Read the README)
# sh configure –prefix/usr/local/opt/ rrdtool-1.0.46
# make
# make install
# make site-perl-install
# ln –s /usr/local/opt/rrdtool-1.0.46 /usr/local/rrdtool
# rm –fr /usr/local/opt/tarballs/rrdtool-1.0.46

# cd /usr/local/opt/tarballs
```

© SANS Institute 2004, Author retains full rights.

#wget "http://www.deadcat.net/download.php?fileid=82&filename=larrd-0.43c.tar.gz&location=1"
tar -xzvf larrd-0.43c.tar.gz
cd larrd-0.43c
perl install --bbhome /usr/local/bb --larrdhome /usr/local/opt/larrd-0.43c
rm –fr /usr/ local/opt/tarballs/ larrd-0.43c
ln -s /usr/local/opt/larrd-0.43c/ /usr/local/larrd
ln -s /usr/local/larrd/ /usr/local/bb/ext/larrd
chown brother.brother /usr/local/bb/ext/larrd
mkdir /usr/local/larrd/tmp
chown brother.apache /usr/local/larrd/tmp
chmod 755 /usr/local/larrd/tmp
mv /larrd-grapher.cgi /larrd-graphs.cgi /monlaa.cgi /www/cgi-bin/
chown root.root /www/cgi-bin/larrd-graph* /www/cgi-bin/monlaa.cgi

Edit the larrd-config file located in /usr/loca/larrd to include the tests you want run on this machine.

Larrd is now installed and needs to be added to BB as an extension which can be done via BBConfig. Edit bb-config and include “ext: larrd/larrd.pl” under the section for this host and then regenerate the bb configuration files by running /usr/local/bin/bbconfigure and restart the BB server “/usr/local/bb/runbb/sh restart”

Within 5-10 minutes the BB display should start to generate graphs on service sub pages and a new column called “trends” will appear on the main page. In the event of problems see the LARRDOUT file located in /usr/local/bb. These graphs display hourly, daily, weekly and monthly trends including CPU load, Disk utilization TCP connections and process, more tests can also be downloaded from www.deadcat.net.

This information can be invaluable to the Administrator as it shows when a machine may need to be upgraded due to CPU load, disk utilization or memory load. Over time It can show irregularities in network traffic and processes which can assist in indicating a broadcast storm or a compromise.

7.7.2 BBGen Installation

BBgen 2.15 offers high performance replacements and enhancements for many BB components. This package requires the use of fping, a utility that tests more than one machine at a time for connectivity in a round robin fashion. To install fping follow these instructions:-

cd /usr/local/opt/tarballs/
http://www.fping.com/download/fping.tar.gz
tar -xzvf fping-2.4b2.tar.gz
cd fping-2.4b2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# ./configure
# make
# make check
# make install
```

To ensure the installation succeeded, run *ping yahoo.com telus.net msn.com* as root, you should get the output below:-

```
# fping yahoo.com telus.net
yahoo.com is alive
telus.net is alive
```

The install bbgen we first need to download and compile the source.

```
# cd /usr/local/opt/tarballs
# wget http://www.deadcat.net/download.php?fileid=772&filename=bbgen-2.15.tar.gz&location=28
# tar –xzvf bbgen-2.15.tar.gz
# cd bbgen-2.15
# ./configure
# make
# make install
```

Some of the new scripts are not automatically moved in case the originals were modified. Also install the “patch” rpm to complete the installation, which can be achieved with the following instructions:

```
# mv /usr/local/bb/bin/bb-display.sh /usr/local/bb/bin/bb-display.bak
# cp bb-display.sh.SAMPLE /usr/local/bb/bin/bb-display.sh
# chmod 755 /usr/local/bb/bin/bb-display.sh
# mv /usr/local/bb/bin/bb-network.sh /usr/local/bb/bin/bb-network.bak
# cp bb-network.sh.SAMPLE /usr/local/bb//bin/bb-network.sh
# chmod 755 /usr/local/bb/bin/bb-network.sh
# cd /usr/local/bb
# yum install patch
# patch -p0 < /usr/local/opt/tarballs/bbgen-2.15/bbpatches/1.9e-server/bbd-background.patch
# patch -p0 </usr/local/opt/tarballs/bbgen-2.15/bbpatches/1.9e-server/bbd-features.patch
# /usr/local/bb/runbb.sh stop
# /usr/local/bbc/runbb.sh stop
#cd src
# make
# make install
# cd /usr/local/bbc
# patch -p0 < /usr/local/opt/tarballs/bbgen-2.15/bbpatches/1.9e-client/bbd-features.patch
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# cd src
# make
# make install
```

Before restarting BB, add suid permission to the fping utility and inform BB of its location. This can be done with the below command:-

```
# echo “FPING=/usr/local/sbin/fping; export FPING” >>
/usr/local/bb/etc/bbsys.local
# chmod +s /usr/local/sbin/fping
```

You can now start both the BB Server and Client and within 5 minutes a new display page should be generated which includes 3 new columns and dramatically increases the speeds of testing.

7.7.3 Maint.pl Extension Script

The final extension of this paper outlines a tool which allows the administrator to disable or enable tests by machine. This can be used to schedule all notification alerts and tests to be disabled when a machine is down for maintenance. It can also be used to disable one or multiple tests from a machine if needed. Installation is simple and can be performed with:-

```
# cd /usr/local/opt/tarballs
# wget
http://www.deadcat.net/download.php?fileid=735&filename=maint.pl.v2.6.
1&location=3
# cp maint.pl.v2.6.1 /www/cgi-bin
# chown root.root /www/cgi-bin/maint.pl
# chmod 755 /www/cgi-bin/maint.pl
```

The file also needs to be edited to chage the first line from “#!/usr/local/bin/perl –wT” to “#!/usr/bin/perl –wT”. To view this page point a browser to the FQDN of this host and add /bb/cgi-bin/maint.pl to complete the URL.

NOTE: This page allows for tests and notification of alerts to be disabled from any valid user account on the system. It is highly recommended to only deploy this page once digest authentication in the apache configuration is enabled and working.

7.7.4 Extension Recommendations

Now that the Monitoring Server infrastructure is in place it is a great time to research other extensions that can be added before deploying clients. As already noted, a great resource for extension scripts is located at www.deadcat.net, as well as the various BB mailing lists which can be found at www.bb4.com. Although installation of the below extensions are beyond the scope of this paper

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

it is recommended to at least research whether they can be utilized within your organization.

Recommended Extensions	Description
• bb-sulog.tgz	• Monitors successful/failed su activity
• Tripwire	• Integrate tripwire reports with BB
• aide-0.7.tar.gz	• Integrate AIDE reports with BB
• ext-snort	• Integrate Snort reports if logging to MYSQL with BB,
• bb-memory-3.0.tar.gz	• Extension script for monitoring memory and swap on Unix- and Windows-based Big Brother clients
• bb-ntp.sh	• Test NTP on various machines. Warns when time drifts too far.
• bb-iostat.sh	• performance checks using vmstat and iostat
• MRTG	• This allows the BB server to poll SNMP enabled network interfaces to gather bandwidth usage statistics. These statistics are then graphed using rrdtools very similar to Larrd. The bb-mrtg extension script can also be configured to alert Administrators when an interface reaches a predefined bandwidth maximum or minimum limit.

7.8 Start-up Script

Before moving onto deploying clients it would be advantageous to have both the BB server/client start on boot. This can be done by adding the script in Appendix E to a new file in the /etc/init.d/ directory and then linking the script to run-level 3.

```
# cd /etc/init.d/
# vi bb
insert script on Appendix E to bb file
# chmod +x bb
# ln -s /etc/init.d/bb /etc/rc3.d/S99bb
# ln -s /etc/init.d/bb /etc/rc3.d/K99bb
```

8.0 Security enhancements

Once the BB software has been completed and any other extensions have been added, the system can be further locked down. At a minimum it is recommended to use the *chattr +i* which sets an attribute so the file cannot be deleted, renamed, or links created to it on all critical files that should not change. To

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

remove this attribute when the file legitimately needs updating run "*chattr –i filename*".

Example setting i attribute
chattr +i /etc/passwd /etc/shadow /etc/group /etc/services /etc/httpd/conf/httpd.conf /usr/local/bb/runbb.sh /usr/local/bb/etc/bb-config /usr/local/bb/etc/security /usr/local/bb/etc/bb-hosts

Example: Clearing the i attribute
chattr -i /etc/passwd /etc/shadow /etc/group /etc/services /etc/httpd/conf/httpd.conf /usr/local/bb/runbb.sh /usr/local/bb/etc/bb-config /usr/local/bb/etc/security /usr/local/bb/etc/bb-hosts

It is recommended to also install tripwire or AIDE onto this machine and integrate the reports into the BB client. Unfortunately the tripwire or AIDE installation is beyond the scope of this paper but both can be found using the below links:-

Tripwire: http://www.tripwire.org/
AIDE: http://sourceforge.net/projects/aide

To further increase security on the server the gcc package can be removed or disabled by using either *yum remove gcc* or *bastille –c* respectively.

9.0 Deploying Clients

It is now time to start the client deployment, make sure that you have already configured network testing for each client on the BB Server. This should be done via bb-config file as it will have automatically populate the security file and set extension, messages, cpu and disk tests properly.

* Since compiling the client on new machines is such a trivial process I would not recommend copying the pre-compiled client to other machines. Instead update the original client tar package with the latest configuration files, scp the new archive to client systems and compile the source.

cd/usr/local/opt/tarballs/
tar –xvf BBCLT-bbc1.9e-btf.tar
cp -R -L /usr/local/opt/bb1.9e-btf/etc/bb-*tab* /usr/local/opt/bb1.9e-btf/etc/bb-hosts /usr/local/opt/tarballs/bbc1.9e-btf/etc
cp -R -L /usr/local/opt/bbc1.9e-btf/ext/* /usr/local/opt/tarballs/bbc1.9e-btf/ext
cp /etc/init.d/bb /usr/local/opt/tarballs/BB/bbc1.9e-btf/

Edit start up script /usr/local/opt/tarballs/bbc1.9e-btf/bb and remove all lines with BBHOME. Copy over any additional extension scripts that need to be run on the client machines to the ext directory and then complete the installation:-

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# tar -czvf bbc1.9e.tgz bbc1.9e-btf/
# scp bbc1.9e.tgz username@client1.domainname
# ssh username@client1.domainname
# su – root
# adduser bbaccount
# passwd  bbaccount
# cd /home_of_username
# tar –xzvf bbc1.9e.tgz
# mv bbc1.9e-btf /usr/local/
# ln -s /usr/local/bbc1.9e-btf/ /usr/local/bbc
# chown -R bbaccount.bbaccount /usr/local/bbc*
# mv /usr/local/bbc/bb /etc/init.d/bbc
# ln -s /etc/init.d/bbc /etc/rc3.d/S99bbc
# ln -s /etc/init.d/bbc /etc/rc3.d/K99bbc
# su – bbaccount
$ cd /usr/local/bbc/install
$./bbconfig linux
$ cd ../src
$ make
$ make install
```

The client should now be installed but needs read access to the log files. Check which files this client has been configured to monitor by viewing the bb-msgtab file in /usr/loca/bbc/etc and then give read permission to the bbaccount for these files. Once this has been done start the client and view the BBOUT file for errors and move onto the next clinet.

```
# /etc/init.d/bbc start
```

To monitor Windows NT based servers there is a msi client installation package which can be downloaded from http://bb4.com/download.html. The installation is very straightforward but remember to update the BBPAGER and BBDISPLAY server IP addresses and update the “alias” name to match this machiens name in the bb-config file.

Note: It is recommended in the installation documentation that all bb clients have the same bb-hosts file and that they are updated when changes are made. This has prompted a few automatic solutions that can be found on www.deadcat.net.

10 Conclusion

This paper has detailed the configuration of BB client/server solution using defence in depth practices to protect the confidentiality, integrity and availability of the network monitoring system

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The BB display and BB pager service display and notify administrators of problems based on network and local tests. The information generated, trended and reported by BB is invaluable to the Administrator as it creates an accurate picture of the state of the network and network services, which will ultimately help to increase the confidentiality, integrity and availability of the entire network.

List of References

Apache HTTP Server Documentation Project. “Authentication, Authorization and Access Control”. http://httpd.apache.org/docs-2.0/howto/auth.html

Brown, Robert. “Automating Nightly Updates”. YUM: Yellowdog Updater, Modified. 17 December 2003. http://www.phy.duke.edu/~rgb/General/yum_article/yum_article/node21.html

Bauer, Mick. “Paranoid Penguin: Seven Top Security Tools” February 01, 2004. http://www.linuxjournal.com/article.php?sid=7235

Cartwright, David. “Stateful vs. deep inspection firewalls” . Jan 8th 2004. http://www.computerworld.com/securitytopics/security/story/0,10801,88871,00.html

Cook Craig. “Big Brother Installation and Configuration Guide” 2002-10-11 http://www.deadcat.net/viewfile.php?fileid=462

Fedora Project, “Hardware Requirements.“ Fedora Core 1 Release Notes. 2003. http://fedora.redhat.com/docs/release-notes/

Fedora Project. “Installation-Related Notes” Fedora Core 1 Release Notes. 2003. http://fedora.redhat.com/docs/release-notes/

Fedora Linux. “Repository Mixing Problems“, January 24, 2004. http://www.fedora.us/wiki/RepositoryMixingProblems

Linux Magazine. “Operating System Hardening” August 2003. http://www.linux-magazine.com/issue/33/Operating_System_Hardening.pdf

MyCERT. “MA-063.012004:MyCERT Special Alert- Mass Web Defacements of Malaysian Websites“,19th January 2004, http://www.mycert.org.my/advisory/MA-063.012004.html

Red Hat, “Chapter 15. TCP Wrappers Configuration Files“. Red Hat Linux 9: Red Hat Linux Reference Guide. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-tcpwrappers-access.html

© SANS Institute 2004, Author retains full rights.

Stearns, William, “Adaptive Firewalls with IPtables”
http://www.sans.org/rr/special/adaptive_firewalls.php

Quest Software.” Big Brother System and Network Monitor - License:”. January 1, 2004. http://www.bb4.com/license.html

Appendix A

The mount points specified below are only for guidance. It is recommended to keep the /boot and /var on separate file systems and BB installation on a RAID device but is not necessary.

/dev/sda1	/boot	ext3	150 MB
/dev/sda2	/	ext3	The rest of the disk
/dev/sda3	/var	ext3	2.5 GB
/dev/sda4		swap	512 MB
/dev/sdb1		RAID	5GB
/dev/sdb2		RAID	2GB
/dev/sdc1		RAID	5GB
/dev/sdc2		RAID	2GB
/dev/md0	/usr/local	ext3	5GB
/dev/md1	/www	ext3	2GB

Appendix B

Custom Package Selection.

- Uncheck X-Windows system
- Uncheck Gnome Envrionment
- Uncheck Graphic Internet
- Check “details” under Text Based Internet and deselect all packages except lynx
- Uncheck office Productivity
- Uncheck Sound and Video
- Check Web Server and click on details
  - Uncheck all php moduels, squid and tux
- Check MailServer and click on details
  - Uncheck dovecot
- Check Development tools and click on details
  - Uncheck everything except the three automake
- Uncheck Printing Support
- Check System tools and click on details
  - Uncheck everything except ethereal

Appendix C

OpenSSH configuration file located at /etc/ssh/sshd_config:
Port 22

© SANS Institute 2004, Author retains full rights.

```
Protocol 2
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication no
PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys
RhostsAuthentication no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreUserKnownHosts no

PasswordAuthentication yes
# To disable tunneled clear text passwords, change to no here!
PermitEmptyPasswords no

# Change to no to disable s/key passwords
ChallengeResponseAuthentication no

# Kerberos options
KerberosAuthentication no
KerberosOrLocalPasswd no
KerberosTicketCleanup no

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
```

©SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
PAMAuthenticationViaKbdInt no

X11Forwarding no
PrintMotd yes
PrintLastLog yes
KeepAlive yes
UseLogin no
UsePrivilegeSeparation yes
PermitUserEnvironment no
Compression yes

#MaxStartups 10
Banner /etc/issue
VerifyReverseMapping no

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Appendix D

```
### Section 1: Global Environment
ServerTokens OS
ServerRoot "/etc/httpd"
PidFile run/httpd.pid
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15

## Server-Pool Size Regulation (MPM specific)
<IfModule prefork.c>
StartServers       8
MinSpareServers    5
MaxSpareServers   20
MaxClients       150
MaxRequestsPerChild  1000
</IfModule>

Listen 192.168.0.2:80

# Dynamic Shared Object (DSO) Support
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule headers_module modules/mod_headers.so
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule mime_module modules/mod_mime.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule dir_module modules/mod_dir.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule cgi_module modules/mod_cgi.so

Include conf.d/*.conf
ExtendedStatus On

### Section 2: 'Main' server configuration
User apache
Group apache
ServerAdmin david.neufeld@shaw.ca
UseCanonicalName Off
TypesConfig /etc/mime.types
DefaultType text/plain
DocumentRoot "/var/www/html"
DirectoryIndex index.html
HostnameLookups Off
ServerSignature On

# Default WebSite Configuration

<Directory />
    Options None
    AllowOverride None
</Directory>

<Directory "/var/www/html">
    Options None
    AllowOverride None
    Order deny,allow
    Allow from all
</Directory>

Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons">
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

# Bir Brother WebSite Configuratuin

ScriptAlias /bb/cgi-bin/ /www/cgi-bin/

<Directory "/www/cgi-bin/">
        AllowOverride None
        Options ExecCGI
        Order allow,deny
        Allow from all
</Directory>

Alias /bb "/www/html"
<Directory "/www/html">
        AllowOverride None
        AuthType Digest
        AuthName "Big Brother is Watching"
        AuthDigestFile /www/auth/bb_pw
        AuthDigestDomain /bb
        Require user devaldi brother root

        Options Indexes
        Order allow,deny
        Allow from all
</Directory>


Alias /error/ "/var/www/error/"
<IfModule mod_negotiation.c>
<IfModule mod_include.c>
    <Directory "/var/www/error">
        AllowOverride None
        Options IncludesNoExec
        AddOutputFilter Includes html
        AddHandler type-map var
        Order allow,deny
        Allow from all
        LanguagePriority en es de fr
        ForceLanguagePriority Prefer Fallback
    </Directory>
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
    ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
    ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
    ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
    ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
    ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
    ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
    ErrorDocument 410 /error/HTTP_GONE.html.var
    ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
    ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
    ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
    ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
    ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
    ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
    ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
    ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
    ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
    ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var

</IfModule>
</IfModule>

#deny access to any ht access files
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>

#Logging Features
ErrorLog logs/error_log
LogLevel warn
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
CustomLog logs/access_log combined
```

Appendix E

```
#!/bin/bash
# This shell script takes care of starting and stopping
# the Big Brother Server
export BBHOME=/usr/local/bb
export BBCHOME=/usr/local/bbc
export BBUSER=brother
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
[ -f $BBHOME/runbb.sh ] || echo "BB Server is not installed"
[ -f $BBCHOME/runbb.sh ] || echo " BB Client is not installed"
EXITCODE=1

 # See how we were called.
 case "$1" in
        start)
                # Start daemons.
                su - $BBUSER -c "cd $BBHOME;./runbb.sh start"
                su - $BBUSER -c "cd $BBCHOME;./runbb.sh start"
                ;;
        stop)
                # Stop daemons.
                su - $BBUSER -c "cd $BBCHOME;./runbb.sh stop"
                su - $BBUSER -c "cd $BBHOME;./runbb.sh stop"
                ;;
        status)
                bbpid=`pidof bbd`
                if [ $bbpid != "" ] ; then
                        echo "BB Server is Running"
                        exit
                fi
                ;;
        restart|reload)
                # Restarts BB
                su - $BBUSER -c "cd $BBCHOME;./runbb.sh stop"
                su - $BBUSER -c "cd $BBHOME;./runbb.sh stop"
                su - $BBUSER -c "cd $BBHOME;./runbb.sh start"
                su - $BBUSER -c "cd $BBCHOME;./runbb.sh start"
                #$0 stop
                #$0 start
                ;;
         *)
                echo "Usage: bb {start|stop|restart|reload|status}"
                exit 1
esac
exit 0

#End of Big  Brother startup script
```

© SANS Institute 2004, Author retains full rights.