Testing Guidance Document

Background Material and Suggested Testing Procedures for the SAGE, Inc. BRICKServer® 2 Web Server Appliance

Prepared by:
Louis A. Jurgens, CISSP
SAGE, Inc.
2201 Civic Circle, Suite 1001
Amarillo, TX 79109

15 July 2003

1.0 Executive Summary & System Overview

The BRICKServer ® 2 Secure Web Appliance is a stand-alone, 1U Rack Mount Server developed by SAGE, Inc. 2201 Civic Circle, Suite 1001, Amarillo, Texas 79109. The SAGE web site is located at www.sage-inc.com.

The appliance is designed as an inexpensive ($6,450) secure system for running web sites as well as in-house ftp and mail servers without having to learn complex computer security techniques. It uses a combination of hardware and software embracing SAGE's Process-Based Security™ (PBS) security model to maintain performance and to keep out hackers. It integrates with an existing network between firewall and router or in parallel with the network server behind a firewall. It may be remotely administered using a proprietary administration program that runs on most any Windows 95/98/ME/NT or 2000 platform.

Remote administration is accomplished with two client side applications, the Administration program and the Configuration program. The Administration program allows an administrator to remotely manage many BRICKServer® 2 functions while the Configuration program is used to enter the information the system needs to communicate with the Internet. The client's link to the server incorporates an MD5-based technique as part of initial authentication when logging into the system, followed by a standard AES encryption for the data transfers with the admin and configuration tools.

The client side requires a Windows 95 through Windows XP computer for remote Administration use. The system supports 10Base-T, 100Base-T and 1 Gb connections. A white paper on PBS is available at www.sage-inc.com.

1.1 Benefits

- Thwarts Website Intrusion and Defacement
- Keeps out malicious *insiders* as well as outsiders
- Prevents Data Access or Damage from Buffer Overflows
- Cannot Be Used in Distributed Denial of Service (DDoS) Attacks
- Simple Central Control of All Users
- Integrates With Existing Network and Firewall
- Does Not Require a Security Expert
- Includes Secure Mail & FTP
- Does Not Require a Firewall
- Eliminates security errors introduced by mis-configuration
- Does *not require* constant security patching

1.2 Common Web Server Exploits and SAGE Response

Web site Threats	The BRICKServer® 2 Response
CGI Exploits. Common Gateway Interface (CGI) is a standard for interactions between programs such as Perl scripts and a web server. They are used for login programs, site search engines, to serve up catalog pages, and many other functions. They also are infamous as one of the most common weaknesses that allow hackers to deface websites or download credit card files. These programs, however, are essential to running sophisticated websites. CGI also enable a web server to run programs. Hackers use these, for example, to run shell scripts to deface websites and often take total control of a computer.	The BRICKServer 2 Process-Based Security™ (PBS) does not permit programs that are run in conjunction with the web server to access any service or the operating system unless specifically permitted under the PBS access control list. Web programmers may have to alter their coding style to comply with PBS. However, with PBS a flawed CGI, ASP, or SSI program simply will not run.
ASP exploits. Active Server Pages (ASP) is the Microsoft incarnation of CGI. Currently this is not supported.	
Server side includes (SSI) also enable a web server to run programs. Hackers use these, for example, to run shell scripts to deface websites and often take total control of a computer.	
Weaknesses in the web server itself. About two-thirds of all hacked websites used Microsoft IIS. Others that have (as of 2001) been revealed as inherently vulnerable include Viking, iPlanet, NetSuite, BadBlue, WEBactive, Pi3Web and Savant.	Under PBS, the web server at no time has the power to perform superuser or administrator functions.
Other vulnerable services on the same computer. A common way to break into a website is by compromising one of the services associated with the website. A search of the Bugtraq archives at http://securityfocus.com reveals some of most common exploits of a various number of services that have been used break into computers.	All services on the BRICKServer 2, Web, E-mail (SMTP, POP3) and FTP, run under PBS and essentially are equally secure.
Operating system vulnerabilities. *Unix-type operating systems* were originally conceived of as the "programmer's toolbox." The very power of this programming environment leaves security in a catch-up game. Almost anything is possible, so security strives to deny as much as possible without breaking the operating system. *Windows-type operating systems*, while having a code legacy from Unix, today are all essentially "black boxes" because their source code is secret. Yet today Windows is the world's most-hacked operating system.	With BRICKServer 2, PBS is integrated into the Linux kernel itself. All functions of the operating system require specific authorization in the PBS process control list (PCL). Concepts of "least privilege" are employed throughout. What is not specifically permitted is automatically disabled.

Misconfiguration of the Web server. Apache is a fairly secure web server but only if properly configured. However, this requires the administrator to be able to compile and debug the modules the site requires and understand the options for authentication and log files.	The BRICKServer 2 web server is automatically secure, impossible to configure in an insecure mode, and requires only minutes of training to administer. A robust security policy is built-in.
Failure to Apply Patches. Most web servers require frequent repairs (patches) because hackers publicize new vulnerabilities every day. Unless customers sign up to the relevant security mailing lists, they may not learn that they need to install a patch until it is too late.	If a bug (or vulnerability) is discovered in the BRICKServer 2 appliance, it will typically be fixed automatically by SAGE. A self-installing upgrade to the server is sent over the Internet.
Mis-configuration of the operating system. The default installations of most, if not all, operating systems except BRICKServer® 2 leave them vulnerable to attack.	The BRICKServer 2 operating system requires no special configuration and no skilled operator.
Weak points elsewhere in the network. Many web servers rely upon firewalls to protect them. A user inside the LAN or a hacker who gains access to a computer inside the LAN can circumvent the firewall.	BRICKServer 2 does not rely on a firewall or any other external protection. It is secure as a stand-alone system. Protection comes from within the kernel, not added on.
Denial of Service (attacks that keep people from accessing servers). Attackers will crash a server by sending it malicious input such as malformed packets or unbounded strings (for example, a URL thousands of characters long).	BRICKServer 2 continuously monitors all server processes. Though generally impervious to crashing, if any required process dies, it will be restarted automatically. In the unlikely event that malicious code gains system access, in no case will it be allowed to run by the PBS mechanism.
Distributed Denial of Service Attacks. The second, more difficult and destructive technique is to entirely fill up the Internet connection capacity for the victim server. Hundreds, perhaps thousands of computers attack by sending as many junk packets as possible to the victim network.	No operating system is able to do anything about distributed denial of service attacks. To stop this sort of attack one must determine where the attacking computers are and shut them off from the Internet. However, PBS™ will prevent a BRICKServer® 2 from being used as a zombie system in DDoS attacks.
Buffer Overflow. In a user-based environment, programs are allowed to run under a user I.D. with critical permissions, like root. If the program was compromised with a buffer overflow (this typically allows a hacker to inject his/her own code into the running program), the hacker had unlimited access to the machine and usually launches a shell for further attack.	Though buffer overflow could still allow the injection of hostile code into the running server, that code would not be able to do anything the original server could have done, because the security profile is set up for the program and not inherited from the user that originally launched the program. As an example, a compromised web server would still only be able to read its web pages and execute its CGI scripts.

1.3 Target Markets

- Small to medium sized businesses desiring a secure, inexpensive, easy to set up web server, with e-mail and ftp servers included.
- Use as departmental server where secure method of posting data for employees (or others) is required.
- Web hosting companies and ISPs.
- Can be used as a Trusted Front End for secure access of local database servers.

1.4 TECHNICAL SPECIFICATIONS

OS: Linux kernel with extensive BRICKServer® 2 modifications
Web server: HTTP 1.1 compliant, thttpd/2.16 29feb00 with BRICKServer® 2 Modifications, Server Side Includes (SSI) 1.1 standard.
Scripting Supported: Perl, PHP, Python, TCL
Databases Supported (external): MySQL, PostgreSQL, SQL Server
Mail and FTP: smtp, pop3, and ftp are SAGE-built to RFCs
Encryption: When logging into the Appliance, MD5 hashing is used for initial authentication. AES is used for encryption of data transfers.
Dimension: 1U, 1.75 inches in height.
Hardware: Intel P4 1.8Ghz CPU (or better), 256 MB(or better)S-DRAM, 40GB hard drive (or better), two NICs; 10/100 NIC plus one 10/100/1GB NIC

The Appliance has the following indicator lights on the front panel:

PWR	Power on
HDD	Hard drive activity
LAN	Connected to LAN
10/100	Light indicates NIC eth0 is connected to a 100Base-T LAN

2.0 List of Claims for Testing Purposes

Claim 1 - The system can be installed and initial setup accomplished in less than 20 minutes by any computer-literate person, not necessarily a Sys Admin.

Claim 2 - Web page updates accomplished by simple drag and drop from client (admin) system, local or remote.

Claim 3 - Unauthorized changing of website content is not possible. Nor is it possible to unmount the drive, stop the swap process, maliciously shut down the INIT or Admin programs, maliciously shut down the server, or delete or change a file or its contents.

Claim 4 - System is resistant to buffer overflow attacks.

Claim 5 - Will not allow Trojans to run, even if installation is successful.

Claim 6 - Cannot exploit thttpd (web server application).

Claim 7 - Cannot exploit Port 1088 (remote admin port).

Claim 8 - Cannot exploit FTP errors.

3.0 Suggested Scripts and Configuration Used for Evaluation

3.1 General - The evaluation should consist of three phases; the installation & setup, running selected applications including uploading a web site, and vulnerability testing of BRICKServer® 2's security mechanism.

- *Installation & setup* will test vendor's claim of "20 minute" installation. It will include connection to the (already established) demonstration subnet, installation of IP address in the server, remote admin application installation at the local client machine, and assignment of e-mail names, passwords, and other permissions. The vendor-provided User Administration Guide will be the sole reference document for the installation & setup procedures.

- *Selected applications* testing will consist of mail system, ftp service, and web server testing. Additionally, new web pages will be moved up to the BRICKServer® 2 to test vendor's claim of "drag and drop" page update capability.

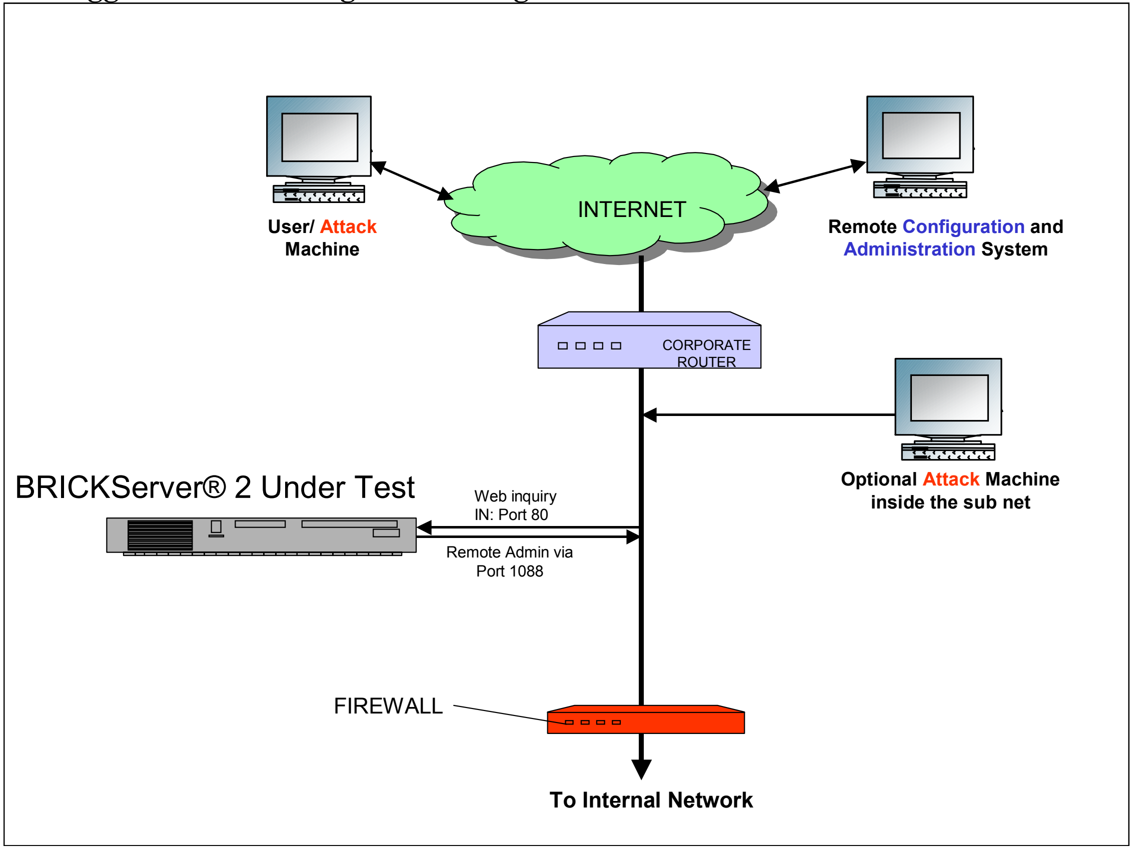
- *Vulnerability* testing will consist of standard penetration techniques such as scanning, o/s and application identification, and insertion of malicious code.

NOTE: All operational testing can be conducted by non-technical, computer literate personnel. Vulnerability testing will require personnel with specialized skills and access to special software. **CAUTION: Standard scanners, e.g., nessus, may give many false positives because of the highly customized Linux kernel, and the modified server modules.** System testers are highly encouraged to run many different exploitation tools against the system.

SAGE will supply the BRICKServer® 2, all other systems and exploitation tools to be provided by tester(s).

SAGE BRICKServer® 2 Appliance

3.2 Suggested Test Configuration Diagram:


User/ Attack Machine
INTERNET
Remote Configuration and Administration System
CORPORATE ROUTER
Optional Attack Machine inside the sub net
BRICKServer® 2 Under Test
Web inquiry IN: Port 80
Remote Admin via Port 1088
FIREWALL
To Internal Network

Suggested Test Configuration

3.3 Suggested Demonstration Scripts

Claim 1: The system can be installed and initial setup accomplished in less than 20 minutes by any computer-literate person, not necessarily a Systems Administrator.

Procedure: Follow written procedures in vendor's manual.

***

Claim 2: Web page updates accomplished by simple drag and drop from client (admin) system, locally or remote.

Procedure: Follow written procedures in vendor's manual.

***

Claim 3 - Unauthorized changing of website content is not possible. Nor is it possible to unmount the drive, stop the swap process, maliciously shut down the INIT or Admin programs, maliciously shut down the server, or delete or change a file or its contents.

Procedure: Run penetration testing at discretion of testers.

***

Claim 4 - System is resistant to buffer overflow attacks.

Procedure: Exploit potential weakness in thttpd/2.16. To mount an attack, access http://www.victim.com/aaaaaaaaaaaaaaaaaaaaaaaaaa… …a. About 800 a's should work. Usually causes DoS, possible buffer overflow. Attacker should then attempt to gain system access and get a malicious program to run.

***

Claim 5: Will not allow Trojans to run, even if installation is successful.

Procedure: Attacker will embed a trojan module in CGI. A PERL script to execute a program using the PERL call ~exec. can be written. Attempt to run /bin/ls. Attempt to run other procedures residing in the cgi-bin directory in an attempt to control the system.

***

Claim 6: Cannot exploit thttpd.

Procedure: (Ref Claim 4, above) Attempt the thttpd buffer overflow exploit. Send filenames of lengths up to approximately 4K to get server to crash.

***

Claim 7: Cannot exploit Port 1088 (remote admin port)

Procedure: Perform a port scan, attempting to get the system to respond to any commands.

***

Claim 8: Cannot exploit FTP errors.

Procedure: Attacker may try >cd/. The command >pwd responds with /, but the system should not accept any commands. This may eventually hang up the FTP shell of the remote terminal.

END