

**PROCESS-BASED SECURITY™
ADDRESSES
THE SANS INSTITUTE & FBI's
TWENTY MOST CRITICAL
INTERNET SECURITY VULNERABILITIES**

Presented By



< process-based solutions >

SAGE, Inc
112 W. 8th Street, Suite #402
Amarillo, Texas 79101
www.sage-inc.com

PHONE: 806-354-8185
FAX: 806-354-8366

Process-Based Security™ (PBS) Addresses the Sans Institute & FBI's Twenty Most Critical Internet Security Vulnerabilities Summary Page

Vulnerabilities Affecting Windows Systems [NOTE: This condition assumes Windows has been re-written with PBS.]		
Will PBS protect me against the following vulnerabilities?	YES	NO
W1. Web Servers & Services	√	
W2. Workstations Service	√	
W3. Windows Remote Access Services	√	
W4. Microsoft SQL Server (MSSQL)	√	
W5. Windows Authentication		√
W6. Web Browsers	√	
W7. File-Sharing Applications	√	
W8. LSAS Exposures	√	
W9. Mail Client	√	
W10. Instant Messaging	√	
Vulnerabilities Affecting UNIX Systems [NOTE: Responses assume PBS is implemented via BRICKServer™.]		
U1. BIND Domain Name System	√	
U2. Web Server	√	
U3. Authentication		√
U4. Version Control Systems		√
U5. Mail Transport Service	√	
U6. Simple Network Management Protocol (SNMP)	√	
U7. Open Secure Sockets Layer (SSL)	√	
U8. Misconfiguration of Enterprise Services NIS/NFS	√	
U9. Databases	√	
U10. Kernel	√	

Process-Based Security™ (PBS) Addresses Vulnerabilities Affecting Windows Systems

[NOTE: This condition assumes Windows has been re-written with PBS.]

W1. Web Servers & Services

- a. Default installations of various HTTP servers on Windows platforms have proven vulnerable to serious attacks.
- b. HTTP servers include IIS, Apache, and SunOne.
- c. Most web servers include sample applications not designed to operate securely in a production environment.

PBS controls what servers and services are allowed to access through the access control list.

W2. Workstation Service

- a. Windows workstation service is responsible for processing user requests to access resources.
- b. The service determines if the resource resides on the local system or on a network share system and routes the user request.

PBS will determine whether access to the resources is needed by specific authorization assigned to the specific user by the administrator.

W3. Windows Remote Access Services

- a. Windows Operating Platforms support a variety of different networking methods and technologies such as NETBIOS Network Shares, Anonymous Logon NULL sessions, remote registry access, and remote procedure calls. These MS specific network technologies are notoriously insecure or misconfigured.
- b. Attackers can exploit these networking methods to compromise the system or form the basis for adjusting file association and permissions to enable malicious code.

PBS would protect all applications on a process level by applying the rules of least privilege.

W4. Microsoft SQL Server (MSSQL)

- a. SQL server contains several serious vulnerabilities.
- b. Remote attackers can exploit sensitive information, alter databases, compromise SQL servers, or compromise server hosts.

PBS would not allow the SQL server to be compromised.

W5. Windows Authentication

- a. Most systems are configured to use passwords, passphrases, and security codes as user authentication.
- b. User identifications are easy to acquire.
- c. Compromised authentication codes are an opportunity to explore a system undetected.
- d. The operating system or additional software creates administrative accounts with weak or nonexistent authentication systems.

PBS cannot protect against weak password, passphrases, or security code situations.

W6. Web Browsers

- a. Windows Internet Explorer has critical vulnerabilities.
- b. A malicious web administrator can design web pages to exploit these vulnerabilities.
- c. The vulnerabilities can be categorized into multiple classes.
- d. The consequences may include disclosure of cookies, local files or data, execution of local programs, download and execution of arbitrary code or complete takeover of the vulnerable system.

PBS would prevent malicious code from executing on the system.

W7. File-Sharing Applications

- a. Peer to Peer File Share Programs (P2P) are user mode applications used to download and distribute many types of data such as music, videos, graphics, text source code, and proprietary information.
- b. Often, the data is either of questionable nature or is copyrighted.
- c. P2P communications consists of requests, replies, and file transfers.
- d. A poorly configured P2P client can provide unauthenticated access to your entire network by sharing mapped drives through the P2P application.

PBS can restrict the file sharing program from running. If **PBS** allows the program to run, the table for the file sharing program can be restricted to a safe location for the type of files being shared.

W8. LSAS Exposures

- a. Windows Local Security Authority Subsystem Service (LSAS) contains critical buffer overflow which can be exploited.
- b. LSAS plays an important role in system authentication and directory functionality. It is here the logging function can be overflowed leading to full system compromise.

PBS does not have such buffer overflow potentials. With **PBS** implemented, logging functions cannot be overflowed thus eliminating full system compromises.

W9. Mail Client

- a. Microsoft has developed usable and intuitive email and information management solutions through Microsoft Outlook and Outlook Express.
- b. The embedded automation features are at odds with the built-in security controls (often disregarded by end-users).
- c. Attackers exploit the embedded features giving rise to e-mail viruses, worms, and malicious code to compromise the local system.

PBS does not protect against Mail Client in its current implementation, but if Mail Client was properly modified to run in a PBS environment, PBS would eliminate these vulnerabilities, though some functionality might be lost.

W10. Instant Messaging

- a. Instant Messaging (IM) technology has matured to a core Windows Operating System capability used for business communication, collaboration, and operational support.
- b. IM is being integrated into the operating system itself which can pose a direct security threat to organizations that have acceptable use policies or secure operational frameworks which deny the use of this technology.
- c. Attack scenarios for IM vulnerabilities can come in the form of remotely executed buffer overflows, URI/malicious link based attacks, file transferring vulnerabilities, or Active X exploits.

PBS does not address instant messaging installed at the operating system level as described above. However, a properly implemented version of PBS, correctly integrated with the IM code would eliminate these vulnerabilities.

Process-Based Security™ (PBS) Addresses Vulnerabilities Affecting Unix Systems

U1. BIND Domain Name System

- a. The most widely used implementation of Domain Name Service (DNS), the critical method used to locate systems on the Internet without knowing the IP address
- b. 50% of all DNS servers run vulnerable versions of BIND.
- c. Outdated BIND versions include buffer overflow exploits used to gain unauthorized access.

PBS does not directly address BIND. However, PBS allows setup of system resources needed for a program. If the program is compromised and new code introduced, the new code can only access resources authorized by the original program.

U2. Web Server

- a. Installations of various HTTP servers on UNIX platforms have proven vulnerable to attacks.
- b. HTTP servers include Apache and the Sun Java System.
- c. Most web servers include applications not regularly maintained.

PBS controls what servers and services are allowed to access through the access control list.

U3. Authentication

- a. Most systems are configured to use passwords as user authentication.
- b. User identifications are easy to acquire.
- c. Compromised passwords are an opportunity to explore a system undetected.
- d. The operating system or additional software creates administrative accounts with weak or nonexistent passwords

PBS cannot protect against weak password situations.

U4. Version Control Systems

- a. Version control systems provide tools to manage documents or source code and facilitate multiple users to concurrently work on the same set of files.
- b. Concurrent Versions System is the most popular source code control system being used in Linux/Unix environments.
- c. An attacker with access could infect source files, and when developed software is distributed, could compromise a large number of systems.

PBS cannot protect against social engineering if an attacker has permission to access certain functions. **PBS** will defend against any unauthorized access.

U5. Mail Transport Service

- a. Mail Transport Agents (MTA) are the servers responsible for getting email from the sender to the recipient.
- b. Sendmail is the most widely-used UNIX based MTA.
- c. Widespread use makes it a prime target for attackers.
- d. Risks presented by running Sendmail:
 1. Privilege escalation caused by buffer overflows.
 2. Improper configuration allowing your machine to be a relay for electronic mail from other machines.

BRICKServer™ does not use Sendmail. However, in the **PBS** environment, access to system resources through Sendmail, or any other mail server application is limited to only those resources authorized by system administration.

U6. Simple Network Management Protocol (SNMP)

- a. SNMP is widely used by network administrators to monitor and administer all types of network-connected devices.
- b. SNMP uses an unencrypted “community string” as its only authentication mechanism.
- c. Attackers use this vulnerability to reconfigure or remotely shut down devices.

PBS currently does not recognize or allow SNMP strings thus eliminating access to the system.

U7. Open Secure Sockets Layer (SSL)

- a. Open SSL is a popular package to add cryptographic security to applications communicating over a network.
- b. Many programs other than Apache have been modified to use Open SSL for security.
- c. Applications use Open SSL to provide cryptographic security for a connection. As a result, exploiters target the application rather than the Open SSL.

PBS limits application authorization; as a result, exploiters would be limited to attacking only application areas. Attackers would not be allowed outside the boundaries of the application.

U8. Misconfiguration of Enterprise Services NIS/NFS

- a. Network Information Service (NIS) is a set of services working as a database service to provide location information to other network services.
- b. Network File Systems (NFS) is a service designed to share files among UNIX systems over a network.
- c. Security problems with both services (buffer overflows, DOS, and weak authentication) have made them frequent targets of attack.

PBS will limit the damage of NIS/NFS's but these applications must be improved before implementation to control attacks.

U9. Databases

- a. Databases are the elements of Electronic Business, Financial, Banking and Enterprise Resource Planning systems, and include critical information from partners, customers, and employees.
- b. Database management systems are collections of programs which store, modify, and extract information from databases.
- c. Database systems are port addressable, meaning anyone with readily available query tools can attempt to connect directly to the database, bypassing security mechanisms used by the operating system.

PBS does not protect against weak database applications. However, PBS will stop system levels attacks used to gain access to the dbms.

U10. Kernel

- a. The kernel is the core component of the operating system.
- b. The kernel has privileged access to all aspects of the system.
- c. Kernel vulnerabilities include denial of service, execution of arbitrary code with system privileges, unrestricted access to the file system, or root level access.
- d. Kernel vulnerabilities can be exploited remotely.

PBS cannot protect against a compromised kernel, but the very nature of PBS redefines what is allowed in the kernel, thus preventing compromise and stopping attacks at the kernel level.