

Confidential Information

The following report contains confidential information, do not distribute, email, fax or transfer via any electronic mechanism unless it has been approved by our security policy. All copies and backups of this documents should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is ground for termination.

Executive Summary

On 28/10/2009 6:08:53 Shadow Security Scanner performed a vulnerability assessment of 1 system(s) in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

SSS goals in this attack were as follows:
Perform network scan to determine all systems and services within your scan range.

Analysis of those systems and services and perform information gathering techniques.

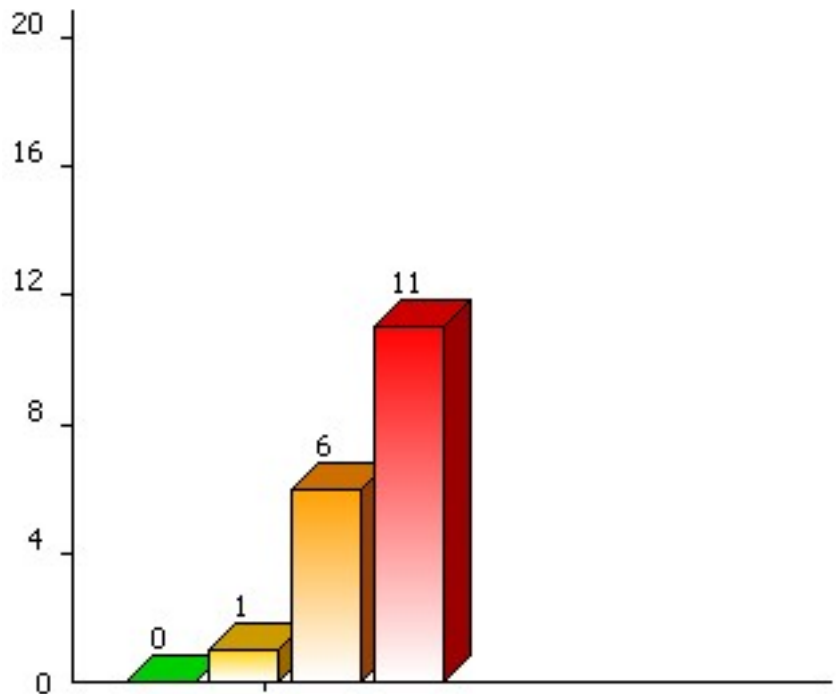
Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.

Generate information on how to fix all found vulnerabilities.

Create security report for your organization.

Your network had 1 low risk vulnerabilities, 6 medium risk vulnerabilities, and 11 high risk vulnerabilities.

Number Of Vulnerabilities By Risk Level



Vulnerability Summary

Introduction

This report was generated on 28/10/2009 6:08:53.
Network security scan was performed using the "UNKNOWN" security policy. Security audits in this report are not conclusive and to be used only as reference, physical security to the network should be examined also. All audits outlined in this report were performed using SSS - Shadow Security Scanner

Top 1-5 Most Vulnerable Hosts

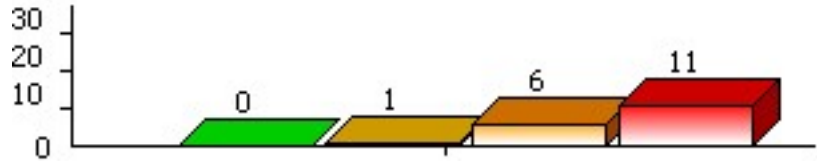


Audits

Audits in SSS the Network Security Scanner are categorized into different sections. The sections are based on the type of services you might be running on your servers and / or workstations.

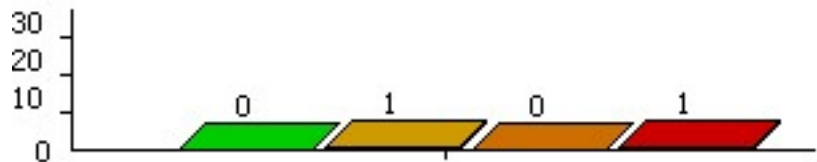
Total Vulnerabilities By Risk Level

The following graph illustrates the total number of vulnerabilities across all machines divided by risk level.



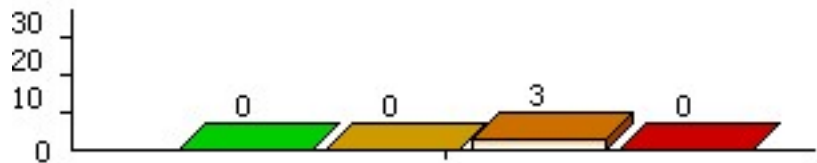
Total Vulnerabilities By Mail Servers Audit

The following graph illustrates the total number of Mail Servers vulnerabilities across all machines divided by risk level.



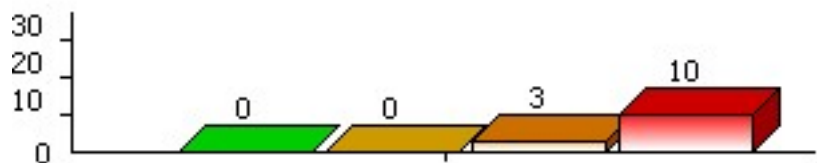
Total Vulnerabilities By SSH Servers Audit

The following graph illustrates the total number of SSH Servers vulnerabilities across all machines divided by risk level.



Total Vulnerabilities By Web Servers Audit

The following graph illustrates the total number of Web Servers vulnerabilities across all machines divided by risk level.



General

Address: 192.168.1.100

This is the IP (Internet Protocol) address of the machine, a single machine might have multiple IP addresses associated with it.

Report Date: 27/10/2009 23:32:04

This is the date and time the scanner started to perform the auditing process. The date and time is reported off the machine local time zone.

Audits

| Mail Servers: SMTP without AuthLogin | |
|--------------------------------------|--|
| Port | 25 |
| Description | An SMTP service supports SMTP without AuthLogin. |
| Risk level | Low |
| How to fix | Install authlogin. |

| Web Servers: Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability | |
|--|---|
| Port | 80 |
| Description | Apache's mod_ssl module is susceptible to a remote denial of service vulnerability. This issue is due to a flaw in the module that results in a NULL pointer dereference, crashing the server. This issue is only present when virtual hosts are configured with a custom 'ErrorDocument' statement for '400' errors, or 'SSLEngine optional'. Depending on the configuration of Apache, attackers may crash the entire Web server, or individual child processes. Repeated attacks are required to deny service to legitimate users when Apache is configured to utilize multiple child processes to handle connections. Apache 2.x versions are affected by this issue. |
| Risk level | Medium |
| How to fix | Upgrade to the current version of Apache. |
| CVE | CVE-2005-3357 |
| BID | 16152 |

| Web Servers: Apache Mod_IMAP Referer Cross-Site Scripting Vulnerability | |
|---|---|
| Port | 80 |
| Description | mod_imap is prone to a cross-site scripting vulnerability. This issue is due to a failure in the module to properly sanitize user-supplied input. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. |
| Risk level | Medium |
| How to fix | Upgrade to the current version of Apache. |
| CVE | CVE-2005-3352 |
| BID | 15834 |

| Web Servers: Apache HTTP Request Smuggling Vulnerability | |
|--|--|
| Port | 80 |
| Description | Apache is prone to an HTTP request smuggling attack. A specially crafted request with a 'Transfer-Encoding: chunked' header and a 'Content-Length' can cause the server to forward a reassembled request with the original 'Content-Length' header. Due to this, the malicious request may piggyback with the valid HTTP request. It is possible that this attack may result in cache poisoning, cross-site scripting, session hijacking and other attacks. This issue was originally described in BID 13873 (Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities). Due to the availability of more details and vendor confirmation, it is being assigned a new BID. |
| Risk level | Medium |
| How to fix | Upgrade to the current version of Apache. |
| CVE | CAN-2005-2088 |
| BID | 14106 |

| SSH Servers: Portable OpenSSH GSSAPI Authentication Abort Information Disclosure Weakness | |
|---|----|
| Port | 22 |

| | |
|-------------|---|
| Description | Portable OpenSSH is prone to an information-disclosure weakness. The issue stems from a GSSAPI authentication abort. Reportedly, attackers may leverage a GSSAPI authentication abort to determine the presence and validity of usernames on unspecified platforms. This issue occurs when Portable OpenSSH is configured to accept GSSAPI authentication. Portable OpenSSH 4.3p1 and prior versions exhibit this weakness. |
| Risk level | Medium |
| How to fix | Upgrade to the latest version of OpenSSH. |
| CVE | CVE-2006-5052 |
| BID | 20245 |

SSH Servers: Portable OpenSSH GSSAPI Remote Code Execution Vulnerability

| | |
|-------------|--|
| Port | 22 |
| Description | Portable OpenSSH is susceptible to a remote code execution vulnerability. The issue derives from a race condition in a vulnerable signal handler. It is reported that under specific conditions, it is theoretically possible to execute code remotely prior to authentication when GSSAPI authentication is enabled. This has not been confirmed and it is reported that the likelihood of a successful exploit of this nature is remote. On non Portable OpenSSH implementations, this same race condition can be exploited to cause a pre-authentication denial of service. This issue occurs when OpenSSH and Portable OpenSSH are configured to accept GSSAPI authentication. |
| Risk level | Medium |
| How to fix | Upgrade to the latest version of OpenSSH. |
| CVE | CVE-2006-5051 |
| BID | 20241 |

SSH Servers: OpenSSH Duplicated Block Remote Denial of Service Vulnerability

| | |
|-------------|---|
| Port | 22 |
| Description | OpenSSH is susceptible to a remote denial-of-service vulnerability. This issue is due to a failure of the application to properly handle incoming duplicate blocks. This issue may be exploited by remote attackers to consume excessive CPU resources, potentially denying service to legitimate users. This issue only occurs when OpenSSH is configured to accept SSH version one traffic. |
| Risk level | Medium |
| How to fix | Upgrade to the latest version of OpenSSH. |
| CVE | CVE-2006-4924 |
| BID | 20216 |

Web Servers: PHP Ini_Restore() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to a 'safe_mode' and 'open_basedir' restriction-bypass vulnerability. Successful exploits could allow an attacker to access sensitive information or to write files in unauthorized locations. This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code, when the 'safe_mode' and 'open_basedir' restrictions are expected to isolate the users from each other. These issues are reported to affect PHP versions 5.1.6, 4.4.4 and prior. Reports indicate that fixes may be available to address this issue; this has not been confirmed. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-4625 |
| BID | 19933 |

Web Servers: PHP Multiple Unspecified Vulnerabilities

| | |
|-------------|---|
| Port | 80 |
| Description | PHP is vulnerable to multiple unspecified vulnerabilities. These issues range from buffer-overflow to cross-site scripting vulnerabilities. The precise nature of these vulnerabilities is currently not known; this BID will be updated as further information becomes available. Some of the issues discussed may be related to other BIDs regarding PHP vulnerabilities. |

| | |
|------------|--|
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | GENERIC-MAP-NOMATCH |
| BID | 17843 |

Web Servers: PHP PHPInfo Large Input Cross-Site Scripting Vulnerability

| | |
|-------------|---|
| Port | 80 |
| Description | PHP is prone to a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-0996 |
| BID | 17362 |

Web Servers: PHP Multiple Safe Mode and Open Basedir Restriction Bypass Vulnerabilities

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to multiple 'safe_mode' and 'open_basedir' restriction-bypass vulnerabilities. Successful exploits could allow an attacker to access sensitive information, or to write files in unauthorized locations. These vulnerabilities would be an issue in shared-hosting configurations where multiple users have the ability to create and execute arbitrary PHP script code, when the 'safe_mode' and 'open_basedir' restrictions are expected to isolate the users from each other. These issues are reported to affect PHP versions 4.4.2 and 5.1.2; other versions may also be vulnerable. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-1608 |
| BID | 17439 |

Web Servers: PHP Multiple Security Bypass Vulnerabilities

| | |
|-------------|---|
| Port | 80 |
| Description | PHP is prone to multiple input validation vulnerabilities that could allow 'safe_mode' and 'open_basedir' security settings to be bypassed. These issues exist in the 'mb_send_mail()' function and various PHP IMAP functions. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-1014 |
| BID | 16878 |

Web Servers: PHP Html Entity Decode() Information Disclosure Vulnerability

| | |
|-------------|--|
| Port | 80 |
| Description | PHP 'html_entity_decode()' function is prone to an information-disclosure vulnerability. This issue arises when a script using the function accepts data from a remote untrusted source and returns the function's result to an attacker. Information that the attacker gathers by exploiting this vulnerability may aid in other attacks. PHP versions prior to 5.1.3-RC1 are vulnerable to this issue. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-1490 |
| BID | 17296 |

Web Servers: PHP Multiple Input Validation Vulnerabilities

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to multiple input validation vulnerabilities. Successful exploits could allow an attacker to write files in unauthorized locations, cause a denial of service condition, and potentially execute code. These issues are reported to affect PHP versions 4.4.3 and 5.1.4; other versions may also be vulnerable. |

| | |
|------------|--|
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-4486 |
| BID | 19582 |

Web Servers: PHP HTMLEntities HTMLSpecialChars Buffer Overflow Vulnerabilities

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to multiple buffer-overflow vulnerabilities because it fails to effectively bounds-check user-supplied input before copying it to an insufficiently sized buffer. An attacker could exploit these issues to have arbitrary code execute in the context of an affected webserver. This may lead to the compromise of the webserver. Failed exploit attempts could cause denial-of-service conditions, denying access to legitimate users. Only limited information is available regarding these issues. This BID will be updated as more information becomes available. PHP 5 is vulnerable to these issues. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-5465 |
| BID | 20879 |

Web Servers: PHP ZendEngine ECalloC Integer Overflow Vulnerability

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to an integer-overflow vulnerability because the application fails to do proper bounds checking on user-supplied data. An attacker can exploit this vulnerability to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely cause denial-of-service conditions. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-4812 |
| BID | 20349 |

Web Servers: PHP Symbolic Link Open Basedir Bypass Vulnerability

| | |
|-------------|--|
| Port | 80 |
| Description | PHP is prone to an 'open_basedir' restriction-bypass vulnerability. Successful exploits could allow an attacker to access sensitive information or to write files in unauthorized locations. This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code; in such cases, the 'open_basedir' restriction is expected to isolate users from each other. This issue is reported to affect PHP versions 4 and 5. |
| Risk level | High |
| How to fix | Upgrade to the current version of PHP. |
| CVE | CVE-2006-5178 |
| BID | 20326 |

Mail Servers: Sendmail Long Header Denial Of Service Vulnerability

| | |
|-------------|--|
| Port | 25 |
| Description | Sendmail is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the Sendmail process causing a denial-of-service. As this issue was reported in OpenBSD's version of Sendmail, information regarding affected Sendmail packages is currently unavailable. This BID will be updated as more information is disclosed. |
| Risk level | High |
| How to fix | Upgrade to the current version of Sendmail. |
| CVE | CVE-2006-4434 |
| BID | 19714 |

Ports

| | |
|--|----------------------|
| 22: SSH - SSH (Secure Shell) Remote Login Protocol | |
| Banner | SSH-1.99-OpenSSH 4.3 |
| Protocol versions | 1.3 1.5 1.99 2.0 |

| | |
|--|--|
| 25: SMTP - Simple Mail Transfer Protocol | |
| Banner | 220 slax.example.net ESMTP Sendmail 8.13.7/8.13.7; Mon, 26 Oct 2009 22:09:53 GMT |
| Protocols | SMTP |
| Heuristic method of detection | Sendmail ESMTP Server 8.11.6 - 8.13.x |

| | |
|--|--|
| 21: FTP - File Transfer Protocol [Control] | |
| Banner | 500 OOPS: could not bind listening IPv4 socket |

| | |
|---|--|
| 80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol) | |
| Protocols | HTTP |
| Version | HTTP/1.1 |
| Server | Apache/2.0.55 (Unix) PHP/5.1.2 |
| Heuristic | The server name was confirmed by heuristic methods |

| | |
|--|-----|
| 110: POP3 - Post Office Protocol - Version 3 | |
| Banner | +OK |
| Protocols | POP |

| | |
|---|--|
| 143: IMAP - Interim Mail Access Protocol v2 | |
| Banner | * OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS AUTH=LOGIN] [192.168.1.100] IMAP4rev1 2004.357 at Mon, 26 Oct 2009 22:10:56 +0000 (GMT) |