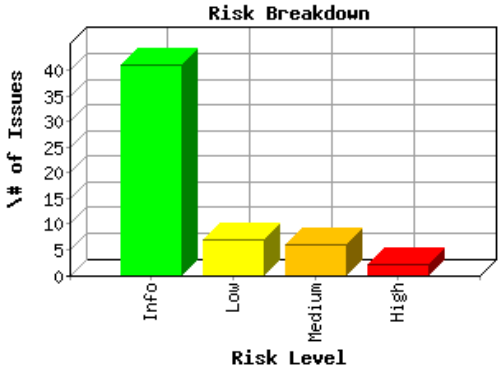
Job Results (ID 1077488)

securityMETRICS®

Executive Summary

Grade: Fail with total risk of 67
Start Date: 2009-06-22 19:34:05
Job Length: 2.74 Hours
Target: 74.86.123.202 / www.pedstest.com
OS Estimate: Linux



SecurityMetrics has determined that this merchant is not compliant with the PCI scan requirement for this computer. The computer **fails** because a risk of 4 or more was found. You may not use the Security Tested logo until the computer passes. Look in the Security Vulnerabilities section below for instructions to reduce your security risk.

Attackers typically use footprinting, port scanning and security vulnerability testing to find security weaknesses on computers. This report provides information on each of these categories.

Footprinting

For public information regarding this IP, which an attacker could use to gain access, see https://www.securitymetrics.com/ipinformation.adp?ip=74.86.123.202

Port Scan

Attackers use a port scan to find out what programs are running on your computer. Most programs have known security weaknesses. Disable any unnecessary programs listed below.

Prot.	Port	Program	Status	Summary
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.
TCP	143	Courier Imapd	Open	Your computer appears to be running Interactive Mail Access Protocol Version 2 (IMAP2). This service generally does not encrypt data or authenticate users. This means the data transmitted by this service may be viewed by others and is not secure.
TCP	2077	None	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	2078	None	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	2082	cPanel httpd 11.24	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	2083	cPanel httpd 11.24	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	2086	cPanel httpd 11.24	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	2087	cPanel httpd 11.24	Open	A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.

TCP	2095	cPanel httpd 11.24	Open	Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.
TCP	2096	cPanel httpd 11.24	Open	Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.
TCP	21	PureFTPd	Open	Your computer allows other computers to connect to it for FTP (file transfer protocol) transfers. If you don't need others to connect to your computer then you should turn off FTP.
TCP	22	ssh	Open	Port 22 is typically used by Secure Shell (SSH) software. Properly configured SSH encrypts all data sent by a remote user who must be authorized to access this computer. Using SSH is a good security practice.
TCP	25	Exim smtpd 4.69	Open	Your computer is running SMTP (Simple Mail Transport Protocol). This can be a security risk since a hacker can verify user names when this service is running. If you do not need to run SMTP then turn it off. If you must run SMTP then be sure to run the latest version.
TCP	26	Exim smtpd 4.69	Open	Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.
TCP	443	Apache httpd 2.2.11	Open	Your computer appears to be running HTTP Secure Socket Layer (SSL) software. This software improves the security of HTTP communication with this server.
TCP	465	Exim smtpd 4.69	Open	Your computer appears to be running a secure version of SMTP (Simple Mail Transport Protocol). This service if configured and maintained properly should improve the security of email messages from this server.
UDP	53	ISC BIND 9.2.4	Open	DNS translates an alphanumeric web address to a numeric IP address. Your ISP typically provides DNS access for you. If you do not require DNS you should turn it off.
TCP	53	ISC BIND 9.2.4	Open	DNS translates an alphanumeric web address to a numeric IP address. Your ISP typically provides DNS access for you. If you do not require DNS you should turn it off.
TCP	80	Apache httpd 2.2.11	Open	Your computer appears to be running http software that allows others to view its web pages. If you don't intend this computer to allow others to view its web pages then turn this service off. There are many potential security vulnerabilities in http software.
TCP	993	Courier Imapd	Open	Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.
TCP	995	Courier pop3d	Open	Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.
ICMP	Ping		Accepting	Your computer is answering ping requests. Hackers use Ping to scan the Internet to see if computers will answer. If your computer answers then a hacker will know your computer exists and your computer could become a hacker target. You should install a firewall or turn off Ping requests.

Security Vulnerabilities

An attacker probes your computer for weaknesses using vulnerability detection tools. The following section lists all security vulnerabilities detected on your computer.

Each vulnerability is ranked on a scale of 0 to 9, with 9 being critical. A risk of 4 or more will fail the test. See https://www.securitymetrics.com/compliance_information.adp for more information.

Prot.	Port	Program	Risk	Summary
TCP	443	https	7	The remote host is using the Apache mod_frontpage module. mod_frontpage older than 1.6.1 is vulnerable to a buffer overflow which may allow an attacker to gain root access. *** Since SMetrics was not able to remotely determine the version *** of mod_frontage you are running, you are advised to manually *** check which version you are running as this might be a false *** positive. If you want the remote server to be remotely secure, we advise you do not use this module at all. **Solution**: Disable this module **Risk Factor**: High CVE : CVE-2002-0427 BID : 4251

TCP	80	http	**7**	The remote host is using the Apache mod_frontpage module. mod_frontpage older than 1.6.1 is vulnerable to a buffer overflow which may allow an attacker to gain root access. *** Since SMetrics was not able to remotely determine the version *** of mod_frontage you are running, you are advised to manually *** check which version you are running as this might be a false *** positive. If you want the remote server to be remotely secure, we advise you do not use this module at all. **Solution**: Disable this module **Risk Factor**: High CVE : CVE-2002-0427 BID : 4251
TCP	443	https	**5**	Synopsis : The remote web server uses a version of PHP that is affected by multiple flaws. Description : According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues : - Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498) - A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names. - Function 'explode()' is affected by an unspecified vulnerability. - It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'. - Function 'xml_error_string()' is affected by a flaw which results in messages being off by one. See also : http://news.php.net/php.internals/42762 http://www.php.net/releases/5_2_9.php http://www.php.net/ChangeLog-5.php#5.2.9 **Solution**: Upgrade to PHP version 5.2.9 or later. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P) CVE : CVE-2008-5498 BID : 33002, 33927 Other references : OSVDB:51031, Secunia:34081
TCP	443	https	**5**	Synopsis : The remote web server contains a PHP script that is prone to an information disclosure attack. Description : Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including : - The username of the user who installed php and if they are a SUDO user. - The IP address of the host. - The version of the operating system. - The web server version. - The root directory of the web server. - Configuration information about the remote PHP installation. **Solution**: Remove the affected file(s). **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
TCP	443	https	**5**	Synopsis : Debugging functions are enabled on the remote web server. Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. See also : http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/288308 http://www.kb.cert.org/vuls/id/867593 **Solution**: Disable these methods. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) **Solution**: Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. Plugin output : SMetrics sent the following TRACE request : ---------- snip ---------- TRACE /SMetrics1072860204.html HTTP/1.1 Connection: Close Host: www.pedstest.com Pragma: no-cache User-Agent: Mozilla/4.75 [en] (X11, U Smetrics) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8 ---------- snip ---------- and received the following response from the remote server : ---------- snip ---------- HTTP/1.1 200 OK Date: Tue, 23 Jun 2009 03:09:08 GMT Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Connection: close Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics1072860204.html HTTP/1.1 Connection: Close Host: www.pedstest.com Pragma: no-cache User-Agent: Mozilla/4.75 [en] (X11, U Smetrics) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8 ---------- snip ---------- CVE : CVE-2003-1567, CVE-2004-2320 BID : 9506, 9561, 11604, 33374 Other references : OSVDB:877, OSVDB:3726, OSVDB:5648

UDP	53	domain	**5**	Synopsis : The remote DNS server is vulnerable to cache snooping attacks. Description : The remote DNS server responds to queries for third-party domains which do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more... See also : For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see: http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
TCP	80	http	**5**	Synopsis : The remote web server uses a version of PHP that is affected by multiple flaws. Description : According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues : - Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498) - A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names. - Function 'explode()' is affected by an unspecified vulnerability. - It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'. - Function 'xml_error_string()' is affected by a flaw which results in messages being off by one. See also : http://news.php.net/php.internals/42762 http://www.php.net/releases/5_2_9.php http://www.php.net/ChangeLog-5.php#5.2.9 **Solution**: Upgrade to PHP version 5.2.9 or later. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P) CVE : CVE-2008-5498 BID : 33002, 33927 Other references : OSVDB:51031, Secunia:34081
TCP	80	http	**5**	Synopsis : Debugging functions are enabled on the remote web server. Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. See also : http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/288308 http://www.kb.cert.org/vuls/id/867593 **Solution**: Disable these methods. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) **Solution**: Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. Plugin output : SMetrics sent the following TRACE request : ---------- snip ---------- TRACE /SMetrics1627760063.html HTTP/1.1 Connection: Close Host: www.pedstest.com Pragma: no-cache User-Agent: Mozilla/4.75 [en] (X11, U Smetrics) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8 ---------- snip ---------- and received the following response from the remote server : ---------- snip ---------- HTTP/1.1 200 OK Date: Tue, 23 Jun 2009 03:09:08 GMT Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics1627760063.html HTTP/1.1 Connection: Keep-Alive Host: www.pedstest.com Pragma: no-cache User-Agent: Mozilla/4.75 [en] (X11, U Smetrics) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8 ---------- snip ---------- CVE : CVE-2003-1567, CVE-2004-2320 BID : 9506, 9561, 11604, 33374 Other references : OSVDB:877, OSVDB:3726, OSVDB:5648
TCP	443	https	**4**	The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d There are several bug in this version of OpenSSL which may allow an attacker to cause a denial of service against the remote host. *** SMetrics solely relied on the banner of the remote host *** to issue this warning **Solution**: Upgrade to version 0.9.6m (0.9.7d) or newer **Risk Factor**: Medium CVE : CVE-2004-0079, CVE-2004-0081, CVE-2004-0112 BID : 9899 Other references : IAVA:2004-B-0006

TCP	443	https	**4**	The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server. An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks. *** SMetrics solely relied on the banner of the remote host *** to issue this warning See also : http://www.openssl.org/news/secadv_20030219.txt http://lasecwww.epfl.ch/memo_ssl.shtml http://eprint.iacr.org/2003/052/ **Solution**: Upgrade to version 0.9.6j (0.9.7b) or newer **Risk Factor**: Medium CVE : CVE-2003-0078, CVE-2003-0131, CVE-2003-0147 BID : 6884, 7148 Other references : OSVDB:3945, OSVDB:3946, RHSA:RHSA-2003:101-01, SuSE:SUSE-SA:2003:024
TCP	80	http	**4**	The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d There are several bug in this version of OpenSSL which may allow an attacker to cause a denial of service against the remote host. *** SMetrics solely relied on the banner of the remote host *** to issue this warning **Solution**: Upgrade to version 0.9.6m (0.9.7d) or newer **Risk Factor**: Medium CVE : CVE-2004-0079, CVE-2004-0081, CVE-2004-0112 BID : 9899 Other references : IAVA:2004-B-0006
TCP	80	http	**4**	The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server. An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks. *** SMetrics solely relied on the banner of the remote host *** to issue this warning See also : http://www.openssl.org/news/secadv_20030219.txt http://lasecwww.epfl.ch/memo_ssl.shtml http://eprint.iacr.org/2003/052/ **Solution**: Upgrade to version 0.9.6j (0.9.7b) or newer **Risk Factor**: Medium CVE : CVE-2003-0078, CVE-2003-0131, CVE-2003-0147 BID : 6884, 7148 Other references : OSVDB:3945, OSVDB:3946, RHSA:RHSA-2003:101-01, SuSE:SUSE-SA:2003:024
TCP	21	ftp	**3**	Synopsis : The remote FTP server allows credentials to be transmitted in clear text. Description : The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack. **Solution**: Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
TCP	80	http	**3**	Synopsis : The remote web server seems to transmit credentials in clear text. Description : The remote web server contains web pages that are protected by 'Basic' authentication over plain text. An attacker eavesdropping the traffic might obtain logins and passwords of valid users. **Solution**: Make sure that HTTP authentication is transmitted over HTTPS. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
ICMP		general/icmp	**1**	Synopsis : It is possible to determine the exact time set on the remote host. Description : The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. **Solution**: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). **Risk Factor**: Low / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) CVE : CVE-1999-0524
TCP		general/tcp	**0**	74.86.123.202 resolves as www.pedstest.com.
TCP		general/tcp	**0**	The following ports were open at the beginning of the scan but are now closed: Port 80 was detected as being open but is now closed This might be an availability problem related which might be due to the following reasons : - The remote host is now down, either because a user turned it off during the scan - A selected denial of service was effective against this host - A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more - This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment. In any case, the audit of the remote host might be incomplete and may need to be done again
UDP		general/udp	**0**	For your information, here is the traceroute from 204.238.82.19 to 74.86.123.202 : 204.238.82.19 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.202 4.71.40.1 4.68.107.190 4.69.132.37 4.69.132.106 4.69.136.138 4.68.19.8 66.228.118.203 66.228.118.190 66.228.118.190 74.86.123.202
TCP		general/tcp	**0**	Synopsis : The remote service implements TCP timestamps. Description : The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed. See also : http://www.ietf.org/rfc/rfc1323.txt **Risk Factor**: None

TCP	110	pop3	**0**	Synopsis : A POP server is listening on the remote port. Description : The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link. See also : http://en.wikipedia.org/wiki/Post_Office_Protocol **Solution**: Disable this service if you do not use it. **Risk Factor**: None
TCP	110	pop3	**0**	A POP3 server is running on this port
TCP	143	imap	**0**	Synopsis : An IMAP server is running on the remote host. Description : An IMAP (Internet Message Access Protocol) server is installed and running on the remote host. **Risk Factor**: None Plugin output : The remote imap server banner is : * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2008 Double Precision, Inc. See COPYING for distribution information.
TCP	143	imap	**0**	Synopsis : There is an unknown service running on the remote host. Description : SMetrics was unable to identify a service on the remote host even though it returned a banner of some type. **Solution**: N/A **Risk Factor**: None
TCP	21	ftp	**0**	An FTP server is running on this port
TCP	21	ftp	**0**	Synopsis : An FTP server is listening on this port. Description : It is possible to obtain the banner of the remote FTP server by connecting to the remote port. **Solution**: N/A **Risk Factor**: None
TCP	25	smtp	**0**	A SMTP server is running on this port
TCP	25	smtp	**0**	Synopsis : An SMTP server is listening on the remote port. Description : The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it. **Solution**: Disable this service if you do not use it, or filter incoming traffic to this port. **Risk Factor**: None
TCP	25	smtp	**0**	For some reason, we could not send the EICAR test string to this MTA.
TCP	443	https	**0**	Synopsis : The remote web server hosts office-related files. Description : This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc. **Solution**: Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials. **Risk Factor**: None
TCP	443	https	**0**	Synopsis : Frontpage extensions are enabled. Description : The remote web server appears to be running with the Frontpage extensions. Frontpage allows remote web developers and administrators to modify web content from a remote location. While this is a fairly typical scenario on an internal Local Area Network, the Frontpage extensions should not be available to anonymous users via the Internet (or any other untrusted 3rd party network). **Risk Factor**: None CVE : CVE-2000-0114 Other references : OSVDB:67
TCP	443	https	**0**	Synopsis : The remote web server contains a mailing list management application written in Python. Description : The remote host is running Mailman, an open source, Python-based mailing list management package. See also : http://www.list.org/ **Risk Factor**: None
TCP	443	https	**0**	A web server is running on this port
TCP	443	https	**0**	This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested you give a high timeout value to this plugin and that you change the number of pages to mirror in the 'Options' section of the client. **Risk Factor**: None
TCP	443	https	**0**	Synopsis : HMAP fingerprints the remote HTTP server. Description : By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options. An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host. Suggestions for defense against fingerprinting are presented in http://acsac.org/2002/abstracts/96.html See also : http://ujeni.murkyroc.com/hmap/ http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf **Solution**: N/A **Risk Factor**: None
TCP	443	https	**0**	Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. **Risk Factor**: None Plugin output : The remote web server type is : Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

TCP	443	https	**0**	Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robotstxt.org/wc/exclusion.html **Solution**: Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material. **Risk Factor**: None Contents of robots.txt : User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /graphics/ Disallow: /files/ Disallow: /cgi-bin/ Other references : OSVDB:238
TCP	443	https	**0**	Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. **Risk Factor**: None
TCP	465	urd	**0**	For some reason, we could not send the EICAR test string to this MTA.
TCP	465	urd	**0**	A SMTP server is running on this port
TCP	465	urd	**0**	Synopsis : An SMTP server is listening on the remote port. Description : The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it. **Solution**: Disable this service if you do not use it, or filter incoming traffic to this port. **Risk Factor**: None
TCP	53	domain	**0**	Synopsis : A DNS server is listening on the remote host. Description : The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses. See also : http://en.wikipedia.org/wiki/Domain_Name_System **Solution**: Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally. **Risk Factor**: None
UDP	53	domain	**0**	Synopsis : A DNS server is listening on the remote host. Description : The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses. See also : http://en.wikipedia.org/wiki/Domain_Name_System **Solution**: Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally. **Risk Factor**: None
UDP	53	domain	**0**	Synopsis : It is possible to obtain the version number of the remote DNS server. Description : The remote host is running BIND, an open-source DNS server. It is possible to extract the version number of the remote installation by sending a special DNS request for the text 'version.bind' in the domain 'chaos'. **Solution**: It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf **Risk Factor**: None Other references : OSVDB:23
UDP	53	domain	**0**	Synopsis : The remote DNS server could be used in a distributed denial of service attack. Description : The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer which is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server. See also : http://isc.sans.org/diary.html?storyid=5713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **Risk Factor**: None
TCP	80	http	**0**	This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested you give a high timeout value to this plugin and that you change the number of pages to mirror in the 'Options' section of the client. **Risk Factor**: None
TCP	80	http	**0**	Synopsis : It is possible to enumerate directories on the web server. Description : This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not. **Risk Factor**: None Plugin output : The following directories were discovered: /_vti_bin, /_vti_log, /_vti_pvt, /_vti_txt, /cgi-bin, /cgi-sys, /downloads, /pipermail, /secure, /dm, /files, /forms, /images, /library, /mailman, /search, /store, /styles, /support, /uploads While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards The following directories require authentication: /_private, /admin Other references : OWASP:OWASP-CM-006
TCP	80	http	**0**	A web server is running on this port
TCP	80	http	**0**	Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. **Risk Factor**: None

TCP	80	http	**0**	Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robotstxt.org/wc/exclusion.html **Solution**: Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material. **Risk Factor**: None Contents of robots.txt : User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /graphics/ Disallow: /files/ Disallow: /cgi-bin/ Other references : OSVDB:238
TCP	80	http	**0**	Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. **Risk Factor**: None Plugin output : The remote web server type is : Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	80	http	**0**	Synopsis : HMAP fingerprints the remote HTTP server. Description : By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options. An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host. Suggestions for defense against fingerprinting are presented in http://acsac.org/2002/abstracts/96.html See also : http://ujeni.murkyroc.com/hmap/ http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf **Solution**: N/A **Risk Factor**: None
TCP	80	http	**0**	Synopsis : The remote web server contains a mailing list management application written in Python. Description : The remote host is running Mailman, an open source, Python-based mailing list management package. See also : http://www.list.org/ **Risk Factor**: None
TCP	80	http	**0**	Synopsis : The remote web server hosts office-related files. Description : This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc. **Solution**: Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials. **Risk Factor**: None
TCP	993	imaps	**0**	Synopsis : There is an unknown service running on the remote host. Description : SMetrics was unable to identify a service on the remote host even though it returned a banner of some type. **Solution**: N/A **Risk Factor**: None
TCP	995	pop3s	**0**	Synopsis : A POP server is listening on the remote port. Description : The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link. See also : http://en.wikipedia.org/wiki/Post_Office_Protocol **Solution**: Disable this service if you do not use it. **Risk Factor**: None
TCP	995	pop3s	**0**	A POP3 server is running on this port

SecurityMetrics PCI SSC Scanning Vendor Compliance Certificate Number: 3707-01-02

This report was generated on Mon Jun 22 22:34:11 2009 MDT