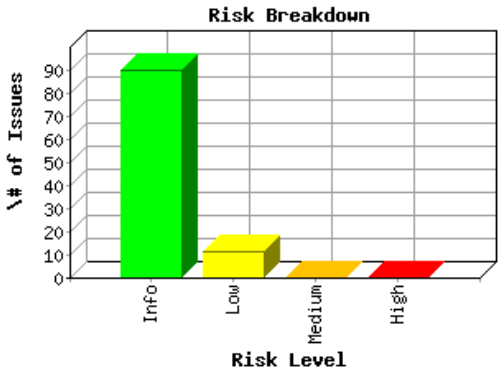
Job Results (ID 1337865)

securityMETRICS®

Executive Summary

Grade: Fail with total risk of 32
Start Date: 2009-12-08 07:18:01
Job Length: 2.36 Hours
Target: 216.22.48.22 / 216.22.48.22
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=216.22.48.22

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	1	tcpmux	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	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.
TCP	111	sunrpc	Open	Local or remote users may be able to execute arbitrary code as root with the privileges of the sunrpc and rpc.statd processes.
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	ProFTPD 1.3.2b	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	OpenSSH 4.3	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	3306	MySQL 5.0.85-community-log	Open	As a security best practice you should not expose database ports externally. Alter your configuration to only allow local access. If you do not need this service, you should turn it off completely.
TCP	443	Apache httpd	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	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	domain	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	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		http/https	4	Possible cross site scripting on https://216.22.48.22/sis/wib/aplic/07mostrarfoto.php Use the following commands to verify this: wp --inject "https://216.22.48.22/sis/wib/aplic/07mostrarfoto.php?Descripcion=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3Elma POST curl -L -k -d "Descripcion=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3Elmagen=" "https://216.22.48.22/sis/wib/aplic/07mostrarfoto.php"| grep "XSS" This website may have other injection related vulnerabilities.
TCP	2077	trellisagt	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)
TCP	2082	infowave	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)
TCP	2086	gnunet	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)
TCP	2095	nbx-ser	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)
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	443	https	3	Synopsis : The remote service allows renegotiation of TLS / SSL connections. Description : The remote service encrypts traffic using TLS / SSL but allows a client to renegotiate the connection after the initial handshake. An unauthenticated remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. See also : http://extendedsubset.com/?p=8 http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.kb.cert.org/vuls/id/120541 http://www.g-sec.lu/practicaltls.pdf https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt **Solution**: Contact the vendor for specific patch information. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N) CVE : CVE-2009-3555 BID : 36935 Other references : OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974
TCP	465	urd	3	Synopsis : The remote service allows renegotiation of TLS / SSL connections. Description : The remote service encrypts traffic using TLS / SSL but allows a client to renegotiate the connection after the initial handshake. An unauthenticated remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. See also : http://extendedsubset.com/?p=8 http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.kb.cert.org/vuls/id/120541 http://www.g-sec.lu/practicaltls.pdf https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt **Solution**: Contact the vendor for specific patch information. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N) CVE : CVE-2009-3555 BID : 36935 Other references : OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974

TCP	993	imaps	**3**	Synopsis : The remote service allows renegotiation of TLS / SSL connections. Description : The remote service encrypts traffic using TLS / SSL but allows a client to renegotiate the connection after the initial handshake. An unauthenticated remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. See also : http://extendedsubset.com/?p=8 http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.kb.cert.org/vuls/id/120541 http://www.g-sec.lu/practicaltls.pdf https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt **Solution**: Contact the vendor for specific patch information. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N) CVE : CVE-2009-3555 BID : 36935 Other references : OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974
TCP	995	pop3s	**3**	Synopsis : The remote service allows renegotiation of TLS / SSL connections. Description : The remote service encrypts traffic using TLS / SSL but allows a client to renegotiate the connection after the initial handshake. An unauthenticated remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. See also : http://extendedsubset.com/?p=8 http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.kb.cert.org/vuls/id/120541 http://www.g-sec.lu/practicaltls.pdf https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt **Solution**: Contact the vendor for specific patch information. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N) CVE : CVE-2009-3555 BID : 36935 Other references : OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974
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**	Synopsis : It was possible to resolve the name of the remote host. Description : SMetrics was able to resolve the FQDN of the remote host. **Solution**: n/a **Risk Factor**: None
UDP		general/udp	**0**	Synopsis : It was possible to obtain traceroute information. Description : Makes a traceroute to the remote host. **Solution**: n/a **Risk Factor**: None
TCP		general/tcp	**0**	The following IP protocols are accepted on this host: 1 ICMP 2 IGMP 6 TCP 17 UDP 41 IPv6 132 SCTP
TCP	1	tcpmux	**0**	The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper
TCP	110	pop3	**0**	A pop3 server is running on this port
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	111	sunrpc	**0**	The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper
TCP	143	imap	**0**	Synopsis : The remote mail service supports encrypting traffic. Description : The remote IMAP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel. See also : http://en.wikipedia.org/wiki/STARTTLS http://tools.ietf.org/html/rfc2595 **Solution**: n/a **Risk Factor**: None
TCP	143	imap	**0**	An IMAP 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. **Solution**: n/a **Risk Factor**: None
TCP	2077	trellisagt	**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. **Solution**: n/a **Risk Factor**: None

TCP	2077	trellisagt	**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. **Solution**: n/a **Risk Factor**: None
TCP	2077	trellisagt	**0**	The following pages are protected by the Basic authentication scheme : /
TCP	2077	trellisagt	**0**	A web server is running on this port
TCP	2082	infowave	**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. **Solution**: n/a **Risk Factor**: None
TCP	2082	infowave	**0**	path = / name = cpsession value = closed version = 1 path = / name = cprelogin value = no version = 1 path = / name = logintheme value = cpanel version = 1
TCP	2082	infowave	**0**	A web server is running on this port
TCP	2082	infowave	**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. **Solution**: n/a **Risk Factor**: None
TCP	2082	infowave	**0**	The following pages are protected by the Basic authentication scheme : /
TCP	2083	radsec	**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. **Solution**: n/a **Risk Factor**: None
TCP	2083	radsec	**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. **Solution**: n/a **Risk Factor**: None
TCP	2083	radsec	**0**	Synopsis : The remote web server does not return 404 error codes. Description : The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Solution**: n/a **Risk Factor**: None
TCP	2083	radsec	**0**	A web server is running on this port
TCP	2086	gnunet	**0**	path = / name = whostmgrsession value = closed version = 1 path = / name = whostmgrrelogin value = no version = 1 path = / name = logintheme value = cpanel version = 1
TCP	2086	gnunet	**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. **Solution**: n/a **Risk Factor**: None
TCP	2086	gnunet	**0**	The following pages are protected by the Basic authentication scheme : /
TCP	2086	gnunet	**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. **Solution**: n/a **Risk Factor**: None
TCP	2086	gnunet	**0**	A web server is running on this port
TCP	2087	eli	**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. **Solution**: n/a **Risk Factor**: None
TCP	2087	eli	**0**	Synopsis : The remote web server does not return 404 error codes. Description : The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Solution**: n/a **Risk Factor**: None
TCP	2087	eli	**0**	A web server is running on this port

TCP	2087	eli	**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. **Solution**: n/a **Risk Factor**: None
TCP	2095	nbx-ser	**0**	A web server is running on this port
TCP	2095	nbx-ser	**0**	path = / name = webmailrelogin value = no version = 1 path = / name = webmailsession value = closed version = 1 path = / name = logintheme value = cpanel version = 1
TCP	2095	nbx-ser	**0**	The following pages are protected by the Basic authentication scheme : /
TCP	2095	nbx-ser	**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. **Solution**: n/a **Risk Factor**: None
TCP	2095	nbx-ser	**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. **Solution**: n/a **Risk Factor**: None
TCP	2096	nbx-dir	**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. **Solution**: n/a **Risk Factor**: None
TCP	2096	nbx-dir	**0**	Synopsis : The remote web server does not return 404 error codes. Description : The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Solution**: n/a **Risk Factor**: None
TCP	2096	nbx-dir	**0**	A web server is running on this port
TCP	2096	nbx-dir	**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. **Solution**: n/a **Risk Factor**: None
TCP	21	ftp	**0**	Synopsis : The remote directory service supports encrypting traffic. Description : The remote FTP service supports the use of the 'AUTH TLS' command to switch from a plaintext to an encrypted communications channel. See also : http://en.wikipedia.org/wiki/STARTTLS http://tools.ietf.org/html/rfc4217 **Solution**: n/a **Risk Factor**: None
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	22	ssh	**0**	An ssh server is running on this port
TCP	22	ssh	**0**	Synopsis : An SSH server is listening on this port. Description : It is possible to obtain information about the remote SSH server by sending an empty authentication request. **Solution**: n/a **Risk Factor**: None
TCP	22	ssh	**0**	Synopsis : A SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Solution**: n/a **Risk Factor**: None
TCP	22	ssh	**0**	Synopsis : Security patches are backported. Description : Security patches may have been 'back ported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. See also : http://www.securitymetrics.com/u?d636c8c7 **Solution**: N/A **Risk Factor**: None
TCP	25	smtp	**0**	For some reason, we could not send the EICAR test string to this MTA.
TCP	25	smtp	**0**	An SMTP server is running on this port Here is its banner : 220-vps.gwt3.info ESMTP Exim 4.69 #1 Tue, 08 Dec 2009 09:54:35 -0430
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	3306	mysql	**0**	A MySQL server is running on this port

TCP	3306	mysql	**0**	Synopsis : A database server is listening on the remote port. Description : The remote host is running MySQL, an open-source database server. The remote database access is restricted and configured to reject access from unauthorized IPs. Therefore it was not possible to extract its version number. **Solution**: n/a **Risk Factor**: None
TCP	3306	mysql	**0**	
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**	Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 04:81:a4:dc:d7:8c:99 Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287 Validity Not Before: Aug 21 20:55:28 2009 GMT Not After : Mar 25 14:04:19 2010 GMT Subject: O=www.sersecoshop.com, OU=Domain Control Validated, CN=www.sersecoshop.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:c7:88:d9:04:85:79:1c:0d:34:f8:8f:ce:02:65: 78:00:89:21:1a:a7:5c:86:5f:e9:cc:69:ca:0a:f5: 03:e6:b6:d1:b9:83:ee:e9:39:fa:91:73:7e:5b:39: 3f:b9:e8:9d:fa:16:7e:3a:87:93:66:f5:2b:d9:59: 95:70:57:9e:1c:c6:3b:36:94:03:1e:20:a6:c6:27: 0d:69:db:a2:a7:9e:fe:6b:03:c3:58:30:01:78:59: 40:24:85:c3:dd:0b:dd:16:bd:7a:62:03:66:cd:fd: 6c:ba:11:63:a3:f3:e2:f7:b8:a9:93:20:e6:a8:34: 83:a9:85:c0:c0:91:b8:42:d1 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: critical CA:FALSE X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Key Usage: critical Digital Signature, Key Encipherment X509v3 CRL Distribution Points: URI:http://crl.godaddy.com/gds1-7.crl X509v3 Certificate Policies: Policy: 2.16.840.1.114413.1.7.23.1 CPS: http://certificates.godaddy.com/repository/ Authority Information Access: OCSP - URI:http://ocsp.godaddy.com/ CA Issuers - URI:http://certificates.godaddy.com/repository/gd_intermediate.crt X509v3 Authority Key Identifier: keyid:FD:AC:61:32:93:6C:45:D6:E2:EE:85:5F:9A:BA:E7:76:99:68:CC:E7 X509v3 Subject Alternative Name: DNS:www.sersecoshop.com, DNS:sersecoshop.com X509v3 Subject Key Identifier: D0:93:11:78:B3:51:02:94:27:57:64:FB:40:7F:6B:48:DC:2D:6B:10 Signature Algorithm: sha1WithRSAEncryption 25:8d:d3:c8:0c:63:15:ae:7a:75:7d:4c:bf:b7:94:6b:1c:10: 01:ad:04:3c:d5:a1:d2:b3:6b:77:f2:8c:73:1e:0b:de:f7:57: 5f:5b:59:0d:ff:68:50:ea:59:fd:44:f8:f1:8b:1b:ec:f6:9c: 86:08:85:1a:d7:fb:ec:41:eb:8c:8c:6c:dd:a1:5d:d7:96:93: 3f:77:84:57:ae:fc:32:54:55:d8:bd:e5:87:ca:99:8d:3d:68: 1d:04:23:99:c1:d5:77:b5:35:86:1e:ac:ca:15:71:19:72:12: 95:ba:04:7d:6b:ce:6d:35:f5:82:9a:0e:0a:41:f4:68:e2:a1: 9f:bf:2e:ae:0b:f1:8a:17:68:2d:e8:02:c9:32:60:c6:e6:e1: 21:63:43:db:91:63:45:18:ac:fc:88:04:47:21:b7:a2:c8:cd: d8:69:ae:ea:5f:a **continued...**
...	...	...	...	**...continued** 5:ac:3c:69:ef:58:51:35:1f:89:5d:05:91: 82:30:6c:45:e9:71:5e:d1:3e:b1:00:c0:22:9b:28:9f:36:42: 6a:a9:cd:12:c8:f2:ba:64:f3:cf:77:a8:6f:43:5d:75:c3:ce: ca:37:bc:52:7d:33:1d:64:77:ef:c4:40:34:ea:ac:be:76:80: 38:55:2f:2f:e9:76:74:bc:11:0e:c6:cb:38:ac:36:f0:7e:f6: 1e:d5:35:fa This TLSv1 server does not accept SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.
TCP	443	https	**0**	Synopsis : The remote service encrypts communications using SSL. Description : This script detects which SSL ciphers are supported by the remote service for encrypting communications. See also : http://www.openssl.org/docs/apps/ciphers.html **Solution**: n/a **Risk Factor**: None
TCP	443	https	**0**	A web server is running on this port through SSL
TCP	443	https	**0**	A TLSv1 server answered on this port
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. **Solution**: n/a **Risk Factor**: None

TCP	443	https	**0**	Synopsis : Some directories on the remote web server are browsable. Description : Miscellaneous SMetrics plugins identified directories on this web server that are browsable. **Solution**: Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do. **Risk Factor**: None
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/ **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. **Solution**: n/a **Risk Factor**: None
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	465	urd	**0**	An SMTP server is running on this port through SSL Here is its banner : 220-vps.gwt3.info ESMTP Exim 4.69 #1 Tue, 08 Dec 2009 09:54:25 -0430
TCP	465	urd	**0**	A TLSv1 server answered on this port
TCP	465	urd	**0**	For some reason, we could not send the EICAR test string to this MTA.
TCP	465			Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 01:67:f9:28:0e Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Validity Not Before: Aug 26 20:41:03 2009 GMT Not After : Aug 26 20:41:03 2010 GMT Subject: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:e1:75:df:65:f4:b8:0c:81:a1:68:d8:af:25:a1: f7:74:85:d0:bb:4c:ae:6b:2a:99:8e:cc:70:df:52: 9b:dd:61:d3:38:1b:03:c1:19:ec:87:bd:b5:1a:85: 57:ee:c4:cf:50:62:98:a4:1c:98:7f:1f:20:e5:9f: 16:45:7a:94:0b:4c:e8:db:4e:35:56:1d:c0:d3:ae: 6c:32:1f:b2:ee:95:22:be:96:10:9f:5c:af:1f:2f: e9:93:70:d2:70:8b:1f:d2:06:d5:2b:7c:62:6a:af: 70:0b:0d:9d:f6:ae:45:23:ab:bf:0a:be:e0:47:c3: 0c:8d:a7:48:b5:41:dc:49:33 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: 8F:87:FA:A3:F5:88:61:C4:7E:4A:C2:F8:7D:6F:25:BF:4A:64:51:33 X509v3 Authority Key Identifier: keyid:8F:87:FA:A3:F5:88:61:C4:7E:4A:C2:F8:7D:6F:25:BF:4A:64:51:33 DirName:/C=US/ST=Unknown/L=Unknown/O=Unknown/OU=Unknown/CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecosh serial:01:67:F9:28:0E X509v3 Basic Constraints: CA:TRUE Signature Algorithm: sha1WithRSAEncryption a3:bd:dc:87:41:bd:88:00:a2:cd:f5:1e:59:d5:d5:19:cb:7f: ef:b3:ff:16:d8:59:65:70:14:5c:82:7d:96:a1:5f:d5:dd:1d: d3:43:8f:ce:52:73:2a:ba:65:b9:2b:07:7f:77:5c:06:2c:13: b1:7a:98:1f:43:1a:23:7f:5f:b9:dc:38:9f:14:2a:b0:10:b8: 67:bc:d3:b1:49:7f:bb:a6:a3:2e:cd:09:c4:5c:16:2f:d4:2b: 41:7b:58:27:2c:89:a2:ca:a7:e7:ea:e8:85:7b:31:00:28:07: 8f:9c:7b:3e:7a:5f:ef:9a:09:60:07:c5:05:e6:43:24:7d:98: 44:36 This TLSv1 server does not accept SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.
UDP	53	domain	**0**	Synopsis : The remote DNS resolver is DNSSEC-aware. Description : The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys. **Solution**: n/a **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 : 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 : The DNS server discloses the remote host name. Description : It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain. **Solution**: It may be possible to disable this feature. Consult the vendor's documentation for more information. **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 : 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**	Synopsis : Some directories on the remote web server are browsable. Description : Miscellaneous SMetrics plugins identified directories on this web server that are browsable. **Solution**: Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do. **Risk Factor**: None
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. **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/ **Solution**: N/A **Risk Factor**: None
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. **Solution**: n/a **Risk Factor**: None
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 : SMetrics crawled the remote web site. Description : 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 that you change the number of pages to mirror in the 'Options' section of the client. **Solution**: n/a **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. **Solution**: n/a **Risk Factor**: None Other references : OWASP:OWASP-CM-006

TCP	993	imaps	0	Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 859624238 (0x333cd32e) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Validity Not Before: Aug 26 20:45:58 2009 GMT Not After : Aug 26 20:45:58 2010 GMT Subject: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:ad:7a:ee:07:a4:53:ce:28:15:8d:06:ae:bb:7d: 18:9a:49:dc:43:97:1a:6c:fb:36:02:98:7f:d6:06: c7:02:02:c9:a9:4c:41:33:d2:45:d4:27:bc:9a:b8: 18:c9:2c:47:9f:d9:cc:25:3a:64:ff:46:79:be:c0: 8c:cc:ec:0b:43:67:c5:59:3a:a6:af:94:64:35:37: 30:8c:11:af:41:a0:b1:fd:dc:50:3b:0a:83:0d:a5: 67:fa:7e:cb:e8:3c:8e:ee:8e:22:9a:ce:67:fd:c5: 5b:e6:7b:e7:db:0f:e4:1c:d1:44:37:88:65:29:d1: 76:aa:4a:bc:da:ce:fa:21:c3 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: C8:B3:6B:AD:7E:31:63:58:63:BE:E8:08:0B:9D:C6:4A:D6:B8:FD:72 X509v3 Authority Key Identifier: keyid:C8:B3:6B:AD:7E:31:63:58:63:BE:E8:08:0B:9D:C6:4A:D6:B8:FD:72 DirName:/C=US/ST=Unknown/L=Unknown/O=Unknown/OU=Unknown/CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecosh serial:33:3C:D3:2E X509v3 Basic Constraints: CA:TRUE Signature Algorithm: sha1WithRSAEncryption 32:7d:53:cd:21:ee:0b:5d:33:50:42:52:09:63:6d:07:fe:0a: 8f:86:34:4c:1f:a8:d6:e8 bb:2e:26:93:f9:b0:fa:e6:8e:e6: 62:47:35:62:a4:f6:1a:0d:7a:00:f0:4d:3e:7c:4f:34:ab:9e: b0:42:cb:80:94:dd:98:ff:01:df:28:70:ea:43:08:61:84:f3: 69:37:44:d9:53:c6:f7:f8 af:42:1f:a3:38:70:6c:09:5a:2d: 6c:01:81:75:61:ba:5a:46:15:87:32:5b:e0:59:d6:7e:aa:fd: 4e:a9:dd:e8:35:f9:2b:37:7e:64:08:09:9b:5d:ce:d2:bd:01: 6a:90 This TLSv1 server does not accept SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.
TCP	993	imaps	0	A TLSv1 server answered on this port
TCP	993	imaps	0	An IMAP server is running on this port through SSL
TCP	993	imaps	0	Synopsis : The remote service encrypts communications using SSL. Description : This script detects which SSL ciphers are supported by the remote service for encrypting communications. See also : http://www.openssl.org/docs/apps/ciphers.html **Solution**: n/a **Risk Factor**: None
TCP	993	imaps	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. **Solution**: n/a **Risk Factor**: None
TCP	995	pop3s	0	A TLSv1 server answered on this port
TCP	995	pop3s	0	Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: -566824399 (-0x21c90dcf) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Validity Not Before: Aug 26 20:45:29 2009 GMT Not After : Aug 26 20:45:29 2010 GMT Subject: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecoshop.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:b5:6d:12:23:15:32:b4:68:78:06:f8:03:41:d2: 6c:e3:4f:cb:8f:bc:3a:26:53:37:09:c3:0e:e2:2c: 4c:8d:d1:cf:83:13:ce:38:5b:72:2c:bb:91:58:f2: 10:30:28:31:f5:20:f5:2a:7d:72:94:cb:a9:54:1b: b7:24:39:4b:07:6a:a9:25:00:67:bd:7e:bc:e2:2f: 01:cc:a9:af:26:66:d8:e9:12:80:a6:d5:31:c1:0e: 31:e9:45:56:d1:cf:1c:a3:90:6a:96:68:e6:38:31: 34:42:b0:1f:da:9d:e5:b3:11:bb:10:0b:ec:9b:b1: 2e:f8:3a:2e:03:e3:75:68:d1 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: D9:8A:52:1A:19:F6:AD:C9:C2:9D:4C:40:62:B9:8A:2D:23:C5:5A:2E X509v3 Authority Key Identifier: keyid:D9:8A:52:1A:19:F6:AD:C9:C2:9D:4C:40:62:B9:8A:2D:23:C5:5A:2E DirName:/C=US/ST=Unknown/L=Unknown/O=Unknown/OU=Unknown/CN=vps.sersecoshop.com/emailAddress=ssl@vps.sersecosh serial:DE:36:F2:31 X509v3 Basic Constraints: CA:TRUE Signature Algorithm: sha1WithRSAEncryption 0a:7f:88:94:0e:11:ef:a8:94:64:e8:55:df:1f:6f:fa:47:96: 61:4c:8e:6f:56:86:6f:1f:14:a3:ef:60:37:25:0b:a1:74:ed: c2:04:a8:a5:fb:e4:a2:b4:e7:01:b5:44:37:90:90:7c:f5:14: a7:88:ff:5a:96:92:a2:4a:13:09:93:46:3b:80:18:5b:cc:ef: 73:76:4a:d3:8c:1d:1d:87:2d:cf:45:c3:3d:9e:62:03:a9:d1: 58:ae:8d:be:b7:24:25:74:42:97:49:b0:48:8d:d6:8a:9d:66: f7:a2:51:5c:71:39:0e:2b:0c:41:d1:da:89:e9:11:a2:70:16: f7:7c This TLSv1 server does not accept SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.
TCP	995	pop3s	0	Synopsis : The remote service encrypts communications using SSL. Description : This script detects which SSL ciphers are supported by the remote service for encrypting communications. See also : http://www.openssl.org/docs/apps/ciphers.html **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 Tue Dec 8 11:20:32 2009 MST