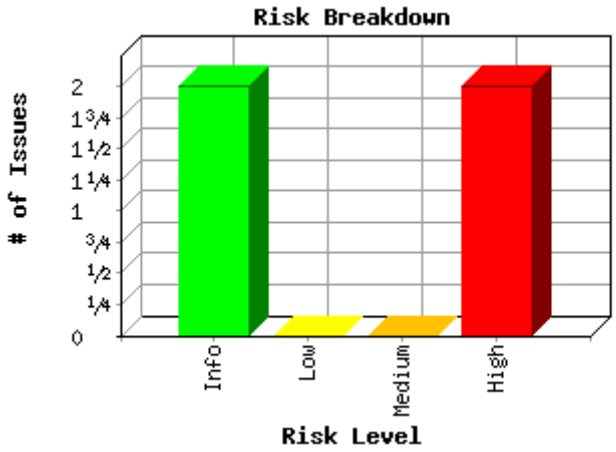
securityMETRICS®

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-11-21**	Target IP: **216.22.48.22**
Test ID: **1311855**	Test Length: **5.69 Hours**	DNS Entry: **216.22.48.22**
Total Risk: **17**	Start Time: **04:11:14**	Finish Time: **09:52:51**
TCP/IP Fingerprint OS Estimate: **Linux**		

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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.	HowTo
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.	HowTo
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.	HowTo
				Your computer appears to be running http software that allows others to view its web pages. If you don't intend this	

TCP	80	Apache httpd	Open	computer to allow others to view its web pages then turn this service off. There are many potential security vulnerabilities in http software.	HowTo
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.	HowTo
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.	
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.	
TCP	2078		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	3306	MySQL 5.0.81-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.	

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
ALL	ALL	general	9	This scan is inconclusive. There is a high probability that some type of firewall or scan-detection software is blocking us from accurately scanning your server. Please configure any firewall or software that would interfere with our scans to allow all traffic from SecurityMetrics - see https://www.securitymetrics.com/scanning .adp If you feel that you have received this notice in error, please contact SecurityMetrics support.
TCP	any port	any service	8	This scan is inconclusive. Though your server had open ports, we were unable to connect to any of them successfully. There is a high probability that some type of firewall or scan-detection software is blocking us from accurately scanning your server. Please configure any firewall or software that would interfere with our scans to allow all traffic from SecurityMetrics - see https://www.securitymetrics.com/scanning .adp If you feel that you have received this notice in error, please contact SecurityMetrics support.
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

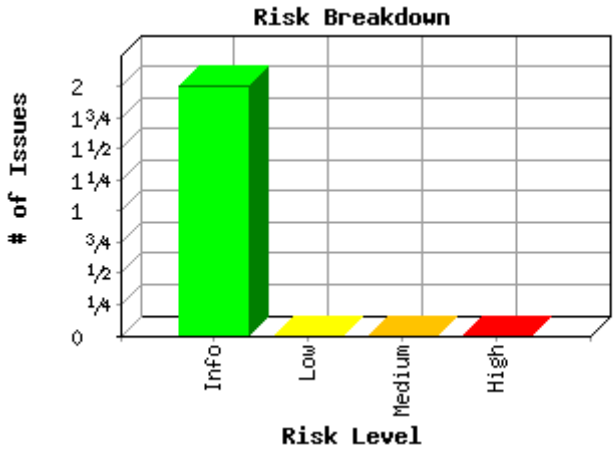
Executive Summary

Test Result: **Pass**	Date: **2009-08-26**	Target IP: **216.22.48.22**
Test ID: **1169771**	Test Length: **3.46 Hours**	DNS Entry: **216.22.48.22**
Total Risk: **0**	Start Time: **11:53:29**	Finish Time: **15:20:56**
TCP/IP Fingerprint OS Estimate:		

SecurityMetrics has determined that Serseco International, LLC. is COMPLIANT with the PCI scan validation requirement for this computer. Congratulations, the computer **passes** because no risk of 4 or more was found.

You may now use the SecurityMetrics Certified logo. Your Site Certification ID is: 407772. Please write this down and proceed to Add Site Certified Logo Instructions.

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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn Off
ICMP	Ping		Denied	Your computer is not answering ping requests. Hackers use Ping to scan the Internet to see if computers will answer. Your computer is not answering, which is a good security practice.	

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
				For your information, here is the traceroute from 204.238.82.18 to

UDP	general/udp	0	216.22.48.22 : 204.238.82.18 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.6.66 154.54.12.122 63.218.83.2 207.58.153.106
TCP	general/tcp	0	216.22.48.22 resolves as vps.blackconnection.net.

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

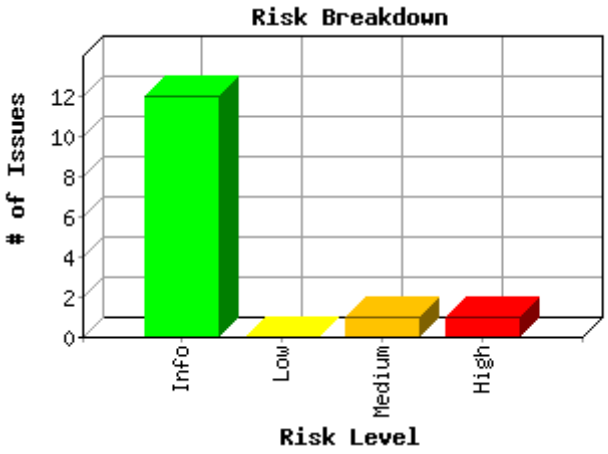
Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-25**	Target IP: **216.22.48.22**
Test ID: **1168442**	Test Length: **4.89 Hours**	DNS Entry: **216.22.48.22**
Total Risk: **13**	Start Time: **15:45:48**	Finish Time: **20:39:04**

TCP/IP Fingerprint OS Estimate: **Linux**

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo

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	smtp	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.	HowTo
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.	HowTo
TCP	80	http	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.	HowTo
TCP	443	https	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	2077		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		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		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	3306	mysql	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	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.	

Security Vulnerabilities Solution Plan

The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities				
Protocol	**Port**	**Program**	**Risk**	**Summary**
ALL	ALL	general	**9**	This scan is inconclusive. There is a high probability that some type of firewall or scan-detection software is blocking us from accurately scanning your server. Please configure any firewall or software that would interfere with our scans to allow all traffic from SecurityMetrics - see https://www.securitymetrics.com/scanning .adp If you feel that you have received this notice in error, please contact SecurityMetrics support.
TCP	8443	pcsync-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		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
TCP		general/tcp	0	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
TCP		general/tcp	0	216.22.48.22 resolves as vps.blackconnection.net.
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		general/tcp	0	The following ports were open at the beginning of the scan but are now closed: Port 8443 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 216.22.48.22 : 204.238.82.19 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.3.17 154.54.6.94 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.22
ICMP		general/icmp	0	Here is the route recorded between 204.238.82.19 and 216.22.48.22 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.5.218 66.28.4.173
TCP	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-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	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-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	8443	pcsync-https	0	A web server is running on this port

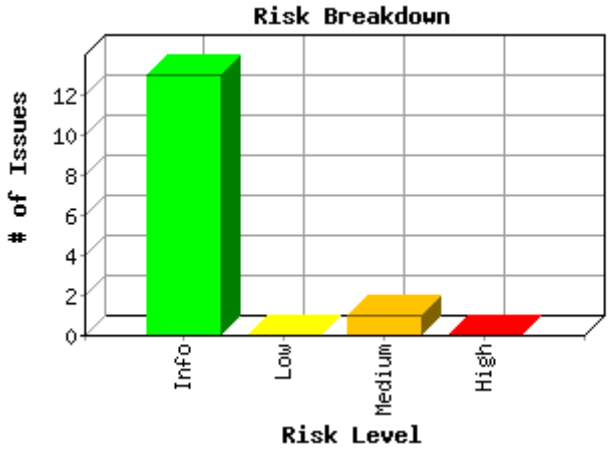
For a list of all vulnerabilities in our knowledge base on this test date click here.

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-24**	Target IP: **216.22.48.22**
Test ID: **1166790**	Test Length: **1.34 Hours**	DNS Entry: **216.22.48.22**
Total Risk: **4**	Start Time: **12:33:55**	Finish Time: **13:54:27**
TCP/IP Fingerprint OS Estimate: **Linux**		

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	Open	DNS translates an alphanumeric web address to a numeric IP address. Your ISP typically provides DNS access for you.	HowTo

				If you do not require DNS you should turn it off.	
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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.	HowTo
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.13	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.	
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.	
TCP	2077		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		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.	
				As a security best practice you should not expose database	

TCP	3306	MySQL 5.0.81-community-log	Open	ports externally. Alter your configuration to only allow local access. If you do not need this service, you should turn it off completely.
TCP	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
TCP	8443	pcsync-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
UDP		general/udp	0	For your information, here is the traceroute from 204.238.82.18 to 216.22.48.22 : 204.238.82.18 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.5.217 154.54.6.66 154.54.12.122 63.218.83.2 207.58.153.106
TCP		general/tcp	0	216.22.48.22 resolves as vps.blackconnection.net.
TCP		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
TCP		general/tcp	0	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
TCP		general/tcp	0	The following ports were open at the beginning of the scan but are now closed: Port 443 was detected as being open but is now closed Port 2086 was detected as being open but is now closed Port 465 was detected as being open but is now closed Port 2087 was detected as being open but is now closed Port 110 was detected as being open but is now closed Port 993 was detected as being open but is now closed Port 22 was detected as being open but is now closed Port 995 was detected as being open but is now closed Port 25 was detected as being open but is now closed Port 2095 was detected as being open but is now closed Port 2096 was detected as being open but is now closed Port 2077 was detected as being open but is now closed Port 2078 was detected as being open but is now closed Port 3306 was detected as being open but is now closed Port 53 was detected as being open but is now closed Port 143 was detected as being open but is now closed Port 8443 was detected as being open but is now closed Port 2082 was detected as being open but is now closed Port 2083 was detected as being open but is 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
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. **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
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
TCP	8443	pcsync-https	0	A web server is running on this port
TCP	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

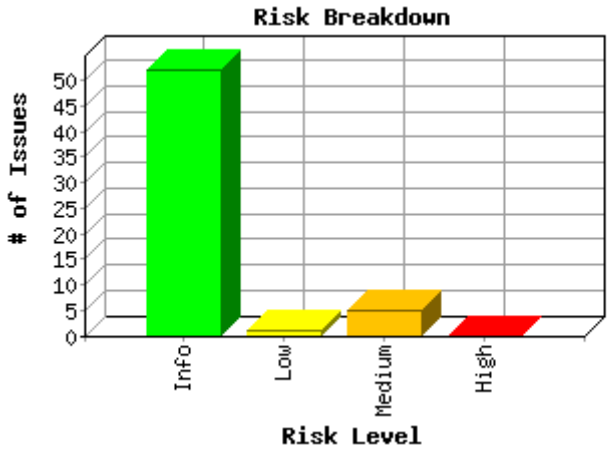
Executive Summary

Test Result: **Fail**	Date: **2009-08-21**	Target IP: **216.22.48.21**
Test ID: **1163874**	Test Length: **1.04 Hours**	DNS Entry: **216.22.48.21**

Total Risk: **25** Start Time: **11:34:15** Finish Time: **12:36:22**

TCP/IP Fingerprint OS Estimate: **Linux**

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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	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.	HowTo
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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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.	HowTo

TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.13	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.	
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.	
TCP	2077		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		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	3306	MySQL 5.0.81-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	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
TCP	443	https	**5**	Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?LWJrP6FvrAMT Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?TppZduK6m9wu Input name : password Page : /. Destination page : sis/wib/aplic/login.php?d3ScigKBnJUO Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?xvPl4d5KkcZn Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?CtdhUHFyBYQj Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?5blik5wYqB9l Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?e5vFXKsa4M7P Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?OccwOHL0I2dM Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?Fe1fC8v3UtSF Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?jYcAONXcq0P5 Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?7bwGTPTZuK5w Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?1DGullORLoh0 Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?PM38LYpY2LZV Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?ZJHqZd9RhGBJ Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?Jqpda7i9WBAk Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?PYD6OS2LuoSD Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?4lcovXa5EGYe Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?E7eb9fBP3FLH Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?YDTIrlMmMoQ8 Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?Cr3HyRm3PGUO Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?mWdfbom0s58a Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?hKCtzTs2Bl9z Input name : password Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?doIhTnOsMDNt Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?MdfBcOuwRPWT Input name : password Page : /. Destination page : sis/wib/aplic/login.php?u3QT7JklDJGc Input name : password Page : /index.htm Destination page :

TCP	80	http	5	sis/wib/aplic/login.php?9onSeJhxUHrg Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?WfWzVcxFWDZT Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?N94QJBsIqVbK Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?e98zGpWcLsRh Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?xjkiD1zaOS2x Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?JpCR4K3NNyYy Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?86MVCXg06GY9 Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?8OaNgSAq8D72 Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?lp5Ek6FNb9bn Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?ZP5RDfC8H1zl Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?ICW8QpK1UF54 Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?ipRdie7wuI15 Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?Zi37huBAYKhr Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?xwa9zotXTA11 Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?fyoP6fKVEETl Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?yVlNfI5T5VTu Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?9CITD9Liyzxu Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?V8GZCaA1wlFR Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?uAlqV4aV7joA Input name : password
TCP	443	https	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-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	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		general/tcp	0	216.22.48.21 resolves as 216.22.48.21.servint.net.
				Synopsis : The remote service implements TCP timestamps. Description :

TCP		general/tcp	0	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		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
TCP		general/tcp	0	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
TCP		general/tcp	0	The following IP protocols are accepted on this host: 0 HOPOPT 1 ICMP 2 IGMP 4 IP 6 TCP 17 UDP 41 IPv6 255
TCP		general/tcp	0	The following ports were open at the beginning of the scan but are now closed: Port 3306 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 204.238.82.17 to 216.22.48.21 : 204.238.82.17 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.3.17 154.54.6.66 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.21
ICMP		general/icmp	0	Here is the route recorded between 204.238.82.17 and 216.22.48.21 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.5.218 154.54.6.57
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	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	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	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	21	ftp	0	An FTP server is running on this port
TCP	22	ssh	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	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. **Risk Factor**: None
TCP	22	ssh	0	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : d5:c5:a3:db:a0:db:aa:f5:35:f7:7c:8f:b9:0a :9a:a0
TCP	25	smtp	0	A SMTP server is running on this port
				Synopsis : An SMTP server is listening on the remote port. Description : The

TCP	25	smtp	0	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	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. It is possible to extract the version number of the remote installation from the server greeting. **Solution**: Restrict access to the database to allowed IPs only. **Risk Factor**: None Plugin output : The remote MySQL version is 5.0.81-community-log
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	A web server is running on this port
TCP	443	https	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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 : 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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 PHP/5.2.10 **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 : 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	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	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
				Synopsis : The DNS server discloses the remote host name. Description : It

UDP	53	domain	0	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
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=5 713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **Risk Factor**: None
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. **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
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 PHP/5.2.10 **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	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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
				Synopsis : The remote web server contains a mailing list management

TCP	80	http	0	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	A web server is running on this port
TCP	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-https	0	A web server is running on this port
TCP	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-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	8443	pcsync-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	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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

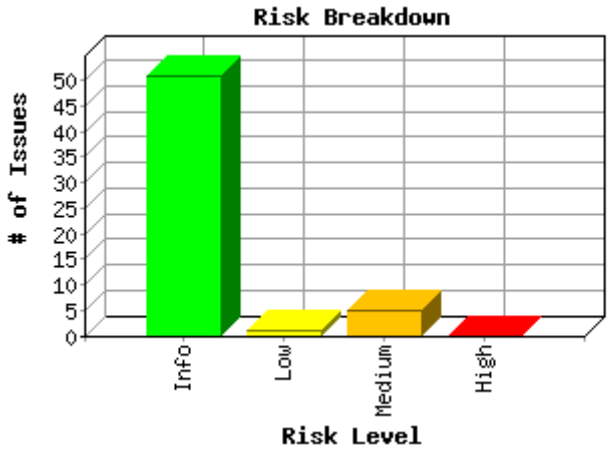
Test Results

Executive Summary

Test Result: **Fail** Date: **2009-08-21** Target IP: **216.22.48.21**

Test ID: **1163502** Test Length: **1.03 Hours** DNS Entry: **216.22.48.21**
Total Risk: **23** Start Time: **04:35:44** Finish Time: **05:37:16**
TCP/IP Fingerprint OS Estimate: **Linux**

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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	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.	HowTo
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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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	HowTo

				vulnerabilities in http software.	
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.13	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.	
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.	
TCP	2077		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		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	3306	MySQL 5.0.81-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.	
		Apache httpd		A program is listening on this port. This helps a hacker to gather information about what is running on this machine	

TCP	4643	2.0.46	Open	and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.
TCP	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
TCP	443	https	**5**	Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?lwaiKjPr6gFE Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?o6aWwRt6mIBs Input name : password Page : /. Destination page : sis/wib/aplic/login.php?whQbv6PEdJDe Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?rL93MdXVGCx9 Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?7m5V3PNqxeIj Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?bXn4hrZO2YHE Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?1ea8hN8f030u Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?H9YSyjyva0gj Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?ZCqTNvmQFGzg Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?zzpHj4er42As Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?cyd2oAcEDIXQ Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?cI47wqMg8YMG Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?HXYlvb88NPiP Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?sMXeDvaf3Udp Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?WFLwwJYYr3nd Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?lz5G9yZll0Kv Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?ZacV6iaSnmEa Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?vdydWb68R2ER Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?re2SUDDtdgFZ Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?FgssIxJ4R7Xo Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?ZUmqMr74L0Nf Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?3RPXxVw32flA Input name : password Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?lEvLN3lPnW51 Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?sCTDQQI1jZCu Input name : password Page : /. Destination page : sis/wib/aplic/login.php?

TCP	80	http	5	9xDHVIrfyQht Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?8Uo8Z3OKfGOa Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?sjuFDXuCKyKf Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?61BvIjfG3KFT Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?DTeias9JSuOW Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?JwMv1zs5WQLE Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?FSMPKku7fowO Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?tRMqIsLReXDW Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?NvRjCcoHv1X6 Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?r1jwGZg25iW1 Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?Us0KWp5tvmq4 Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?aaHDMc63Tgqa Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?tTdbqQBCsPpN Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?yqgAvNBG2mLt Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?pumWSciBvCdc Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?SfeBuJOj0vjl Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?8ks1M3k1oNN6 Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?pw8byb3H6XIr Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?hXQXIz9Gar7m Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?liePwsMbeK3T Input name : password
TCP	443	https	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-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
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	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux

				Kernel 2.4 on Red Hat Enterprise Linux 3
TCP		general/tcp	0	The following IP protocols are accepted on this host: 0 HOPOPT 1 ICMP 2 IGMP 4 IP 6 TCP 17 UDP 41 IPv6 255
UDP		general/udp	0	For your information, here is the traceroute from 204.238.82.18 to 216.22.48.21 : 204.238.82.18 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.5.157 154.54.6.58 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.21
TCP		general/tcp	0	216.22.48.21 resolves as 216.22.48.21.servint.net.
ICMP		general/icmp	0	Here is the route recorded between 204.238.82.18 and 216.22.48.21 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.5.126 154.54.6.93
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		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
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	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	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	21	ftp	0	An FTP server is running on this port
TCP	22	ssh	0	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : d5:c5:a3:db:a0:db:aa:f5:35:f7:7c:8f:b9:0a :9a:a0
TCP	22	ssh	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	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. **Risk Factor**: None
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	25	smtp	0	A SMTP 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. It is possible to extract the version number of the remote installation from the server greeting. **Solution**: Restrict access to the database to allowed IPs

				only. **Risk Factor**: None Plugin output : The remote MySQL version is 5.0.81-community-log
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	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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 PHP/5.2.10 **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 : 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 : 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**	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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	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**	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
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. **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=5 713 **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 : 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 : 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 : 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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 PHP/5.2.10 **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 : 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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
TCP	80	http	0	A web server is running on this port
TCP	8443	pcsync-https	0	A web server is running on this port
TCP	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You

				can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-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	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-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	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	A POP3 server is running on this port
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-20**	Target IP: **216.22.48.21**
Test ID: **1162322**	Test Length: **1.01 Hours**	DNS Entry: **216.22.48.21**
Total Risk: **40**	Start Time: **15:58:18**	Finish Time: **16:59:07**

TCP/IP Fingerprint OS Estimate: **Linux**

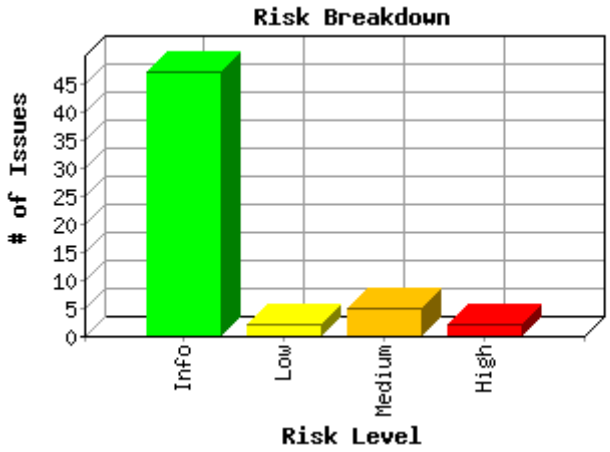
SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation requirement for this computer. The computer **fails** because a risk of 4 or more was found. You may not use the

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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.



Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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	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.	HowTo
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	smtp	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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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.	HowTo
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
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.	HowTo

TCP	443	Apache httpd 2.2.13	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.
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.
TCP	2077		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		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	3306	MySQL	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	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan

The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale

from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	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 might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?AIttDaUBENSP Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?6haGxzMxJSxU Input name : password Page : /. Destination page : sis/wib/aplic/login.php?2GC4U7x6BOJI Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?3RoOt71bmrgm Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?3o3auUEmaGhv Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?EUrFj1OcI3r2 Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?0jTdQzGJdAjN Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?6HwPKNFQTG7v Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?E5OSYqrkxtkJ Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?LKamFv8C3vSE Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?8XUSeSEiOS1m Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?sM7m64lnOxkp Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?tZnErZEe3GzF Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?xblPQKR9XPlU Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?KN7YAiEu7ryp Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?H2JA99GwasCq Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?3UqQjRktfiIf Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?GMPE4DtC63C5 Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?2JsS1u9uEpAn Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?7lWcJe7PrNTl Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?RDnN6qJyz1Gr Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?lGbpvcTsDpLN Input name : password Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0

TCP	80	http	5	(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?cMxmoQHwB7jP Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?bDYI4yjEOlp1 Input name : password Page : /. Destination page : sis/wib/aplic/login.php?ydjp5v4981Ol Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?nmKXbPlP1d5F Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?nNR64qqtKPYG Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?ATF9LUlz6vMY Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?Axn2Ri74wP1r Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?YTVKzXy3h8Jv Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?SXB7wzxVffuS Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?I9C66seVC0g1 Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?NVvuU4gmShkE Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?WAfWQCors5qk Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?8n2RKpN3GpFj Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?PYskvvcHv7dC Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?AbT5jllifOvn Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?ojqvoqTP73Nq Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?dFiwvrkvI4qs Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?fSQBgCoLlV7Q Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?BQf9KspnyOZj Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?5AUE4BwaTDbz Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?FGArb77cOdcY Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?LHCAVbkRb4VV Input name : password
TCP	443	https	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-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	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)
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**	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
ICMP		general/icmp	**0**	Here is the route recorded between 204.238.82.19 and 216.22.48.21 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.5.158 154.54.6.65
TCP		general/tcp	**0**	216.22.48.21 resolves as 216.22.48.21.servint.net.
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		general/tcp	**0**	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
TCP		general/tcp	**0**	The following IP protocols are accepted on this host: 0 HOPOPT 1 ICMP 2 IGMP 4 IP 6 TCP 17 UDP 41 IPv6 255
UDP		general/udp	**0**	For your information, here is the traceroute from 204.238.82.19 to 216.22.48.21 : 204.238.82.19 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.5.125 66.28.4.174 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.21
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	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	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	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	22	ssh	**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	22	ssh	**0**	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : d5:c5:a3:db:a0:db:aa:f5:35:f7:7c:8f:b9:0a :9a:a0
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. **Risk Factor**: None
				Synopsis : Some information about the remote HTTP configuration can be

TCP	443	https	0	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	443	https	0	A web server is running on this port
TCP	443	https	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **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 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	465	urd	0	For some reason, we could not send the EICAR test string to this MTA.
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	A SMTP server is running on this port
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=5 713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **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 : 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 : 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 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. **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. **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. **Risk Factor**: None Plugin output : The remote web server type is : Apache/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **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	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
TCP	80	http	0	A web server is running on this port
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	8443	pcsync-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
				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

TCP	8443	pcsync-https	0	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	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-https	0	A web server is running on this port
TCP	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-20**	Target IP: **216.22.48.21**
Test ID: **1162292**	Test Length: **1.03 Hours**	DNS Entry: **216.22.48.21**
Total Risk: **37**	Start Time: **14:51:30**	Finish Time: **15:53:05**

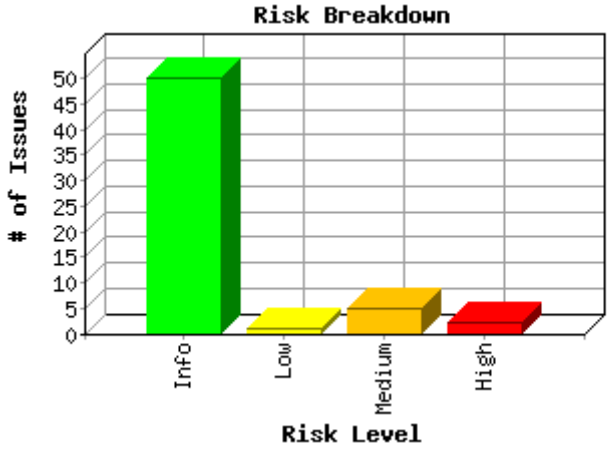
TCP/IP Fingerprint OS Estimate: **Linux**

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.



Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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	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.	HowTo
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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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.	HowTo
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.13	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.
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.
TCP	2077		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		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	3306	MySQL	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	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	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 might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?TyNwq68hV9QL Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?caSf52LuPXuD Input name : password Page : /. Destination page : sis/wib/aplic/login.php?8mxeQ2o6pVbU Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?7KahHsv0Bw3R Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?cRdAWHWUtKz9 Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?Cd6szXCxhdUp Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?LFfM1ZeUr8UE Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?TaE3SGh7Anu1 Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?qd8EOXBZFR1e Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?YbIFhMd0mit5 Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?pQ2p4nhlGfpV Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?CaLibOVkr4bZ Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?hit8FwO0RkAe Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?RVgA7CNAcYj4 Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?m4eUz6tWedVk Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?PjahKbBcxicu Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?kpuDEU7rOcBD Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?Yva2OvcdV3Ag Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?UC8Hka2KGnNK Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?7L1Mn2PBnq42 Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?bXVxRVTmXRu8 Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?snIyQW8Oi0aL Input name : password Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?fOdXkwhInqoN Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?vfWJMqVBslgM Input name : password Page : /. Destination page : sis/wib/aplic/login.php?

TCP	80	http	5	OW5SwqSD72Po Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?vVdS4QPyzPVg Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?PNBMLOtakpsW Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?VBaT3p8pBc76 Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?sNvhdGDsUF4f Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?JfNt1ejtNwLw Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?c0C641Uid2sM Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?0ZAt0lqAG4t8 Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?YSrmE3Yhtbdo Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?p9omVOUpCfjq Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?zXMAxPmxCsAu Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?yAFnxRjcROFm Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?djYW0zofZqTe Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?YTFdxSYHCPX9 Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?s0Yi2itWIHs9 Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?7WeWDx1cH665 Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?PUCSjaSSQr1I Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?PkeYrNXpk1Cn Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?p3Gx0CsGXvZ7 Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?LrPbYGkoqFDY Input name : password
TCP	443	https	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-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
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	216.22.48.21 resolves as 216.22.48.21.servint.net.
				Synopsis : The remote service implements TCP timestamps. Description :

TCP		general/tcp	0	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		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
TCP		general/tcp	0	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
UDP		general/udp	0	For your information, here is the traceroute from 204.238.82.19 to 216.22.48.21 : 204.238.82.19 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.5.125 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.21
TCP		general/tcp	0	The following IP protocols are accepted on this host: 0 HOPOPT 1 ICMP 2 IGMP 4 IP 6 TCP 17 UDP 41 IPv6 255
ICMP		general/icmp	0	Here is the route recorded between 204.238.82.19 and 216.22.48.21 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.3.18 154.54.6.57
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	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	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	21	ftp	0	An FTP 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. **Risk Factor**: None
TCP	22	ssh	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	22	ssh	0	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : d5:c5:a3:db:a0:db:aa:f5:35:f7:7c:8f:b9:0a :9a:a0
TCP	25	smtp	0	A SMTP server is running on this port
TCP	25	smtp	0	For some reason, we could not send the EICAR test string to this MTA.
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	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	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	A web server is running on this port
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **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 : 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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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	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	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
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
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 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
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=5 713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **Risk Factor**: None
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. **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
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **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**	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 : 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 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 : 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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
TCP	80	http	**0**	A web server is running on this port
TCP	8443	pcsync-https	**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. **Risk Factor**: None
TCP	8443	pcsync-https	**0**	A web server is running on this port
TCP	8443	pcsync-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	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-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	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	A POP3 server is running on this port
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-20**	Target IP: **216.22.48.21**
Test ID: **1162067**	Test Length: **1.03 Hours**	DNS Entry: **216.22.48.21**
Total Risk: **59**	Start Time: **08:18:40**	Finish Time: **09:20:32**

TCP/IP Fingerprint OS Estimate: **Linux**

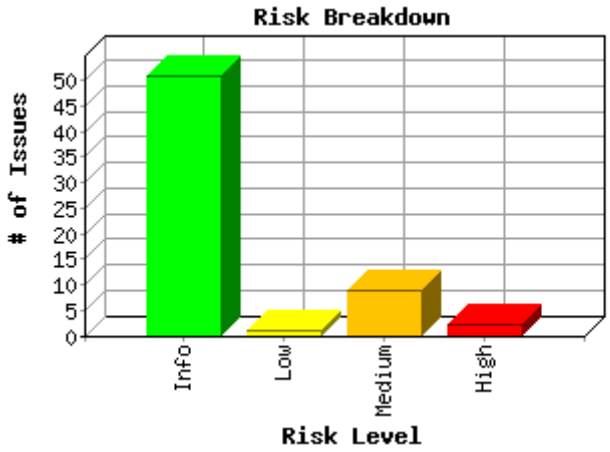
SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation requirement for this computer. The computer **fails** because a risk of 4 or more was found. You may not use the Security Tested logo until the computer passes. Look in the Security Vulnerabilities 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.



Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
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	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.	HowTo
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.	HowTo
UDP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	53	ISC BIND 9.3.4-P1	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.	HowTo
TCP	80	Apache httpd 2.2.13	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.	HowTo
TCP	110	Courier pop3d	Open	Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor.	HowTo
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.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.13	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.
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.
TCP	2077		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		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	3306	MySQL 5.0.81-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	4643	Apache httpd 2.0.46	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	8443	Apache httpd 2.0.46	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.

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	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 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-mirr or/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-2 4 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 /SMetrics1819422761.html HTTP/1.1 Connection: Close Host: 216.22.48.21.servint.net 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: Thu, 20 Aug 2009 14:33:35 GMT Server: Apache/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics1819422761.html HTTP/1.1 Connection: Keep-Alive Host: 216.22.48.21.servint.net 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	5	Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields

TCP	443	https	5	containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?NebzUlw4HSLb Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?qBOH8yLGVQda Input name : password Page : /. Destination page : sis/wib/aplic/login.php?zhYCVXNBxFi8 Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?3QJPdlheBcyE Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?W5Ji2tdrQ2tm Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?P7oDCMB6dKM6 Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?wtbxMP2iLBGD Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?bCamGGpNHxdN Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?TN67DfmF34J0 Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?cEN9jPnBRDnX Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?JTlRHEeaSaYW Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?o61zm6M9cULA Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?1d7U6JPqOk4m Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?r7ndvdRZaJPC Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?Ea4fPstbdbJZ Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?8EhVX9fSRE0S Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?S3RvYPOcpJ75 Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?1qWUIfuGkRc7 Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?R8QjCG1U9JGX Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?YVzEexAVeXqn Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?3audsMaAKqjN Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?wbhwkoJ9A9Ee Input name : password
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-mirr or/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-2 4 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 /SMetrics504288901.html HTTP/1.1 Connection: Close Host: 216.22.48.21.servint.net 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: Thu, 20 Aug 2009 14:33:34 GMT Server: Apache/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: message/http TRACE

				/SMetrics504288901.html HTTP/1.1 Connection: Keep-Alive Host: 216.22.48.21.servint.net 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	80	http	**5**	Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?W4e9iSqRHF6e Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?efK2ZJhDcpeW Input name : password Page : /. Destination page : sis/wib/aplic/login.php?iAzBVtWjqx9W Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?i0AdLLDVMLNJ Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?vmcIjkAHl0J7 Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?jggQTgm2XmWi Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?yZ4AkHKVtneT Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?9ieR5z6mSn9x Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?BSzft26cNy9K Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?pa2gKysKWMcR Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?BZ4TD3HEL6k5 Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?Z9kpG6AwLDpD Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?HAHPGgutnzip Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?CXSE7h4WhfBn Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?FvPXanACdWNq Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?DVSpfusCmahF Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?0I1pxIL33aRT Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?ERViojOr4gWa Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?REd4eA9UJ1A7 Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?9L03lINqZjOD Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?IcvD9HeRM7Lr Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?7LBGCCDCN45z Input name : password
TCP	80	http	**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	**4**	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525,

				OSVDB:24469, OSVDB:42314
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting **Solution**: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-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	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		general/tcp	0	The following IP protocols are accepted on this host: 0 HOPOPT 1 ICMP 2 IGMP 4 IP 6 TCP 17 UDP 41 IPv6 255
ICMP		general/icmp	0	Here is the route recorded between 204.238.82.19 and 216.22.48.21 : 64.90.192.38 206.71.65.42 64.78.227.86 64.78.230.193 38.104.26.154 154.54.5.29 154.54.24.81 154.54.5.158 154.54.6.65
TCP		general/tcp	0	216.22.48.21 resolves as 216.22.48.21.servint.net.
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		general/tcp	0	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Enterprise Linux 3
TCP		general/tcp	0	Remote operating system : Linux Kernel 2.4 on Red Hat Enterprise Linux 3 Confidence Level : 95 Method : HTTP The remote host is running Linux Kernel 2.4 on Red Hat Enterprise Linux 3
UDP		general/udp	0	For your information, here is the traceroute from 204.238.82.19 to 216.22.48.21 : 204.238.82.19 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.203 38.104.26.153 154.54.5.30 154.54.24.82 154.54.5.125 66.28.4.174 154.54.12.122 63.218.83.2 207.58.153.106 216.22.48.21
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	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	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	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	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. **Risk Factor**: None
TCP	22	ssh	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	22	ssh	0	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : d5:c5:a3:db:a0:db:aa:f5:35:f7:7c:8f:b9:0a :9a:a0
TCP	25	smtp	0	For some reason, we could not send the EICAR test string to this MTA.
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	A SMTP 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. It is possible to extract the version number of the remote installation from the server greeting. **Solution**: Restrict access to the database to allowed IPs only. **Risk Factor**: None Plugin output : The remote MySQL version is 5.0.81-community-log
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	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
				Synopsis : Some information about the remote HTTP configuration can be

TCP	443	https	0	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	A SMTP server is running on this port
TCP	465	urd	0	For some reason, we could not send the EICAR test string to this MTA.
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 : 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
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=5 713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **Risk Factor**: None
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. **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
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 : 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	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: /_backup, /cgi-bin, /cgi-sys, /pipermail, /test, /css, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
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/2.2.13 (Unix) mod_ssl/2.2.13 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.10 **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 : 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	A web server is running on this port
TCP	8443	pcsync-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/2.0.46 (Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a **Solution**: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
TCP	8443	pcsync-https	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. **Risk Factor**: None
TCP	8443	pcsync-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	8443	pcsync-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	8443	pcsync-https	0	A web server is running on this port
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

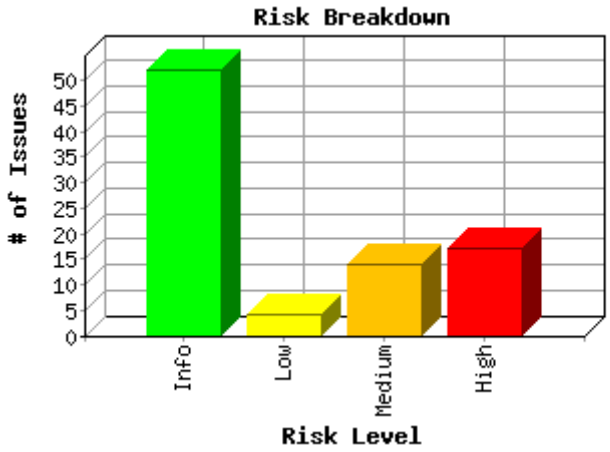
This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.

Test Results

Executive Summary

Test Result: **Fail**	Date: **2009-08-19**	Target IP: **216.22.48.21**
Test ID: **1160466**	Test Length: **1.88 Hours**	DNS Entry: **www.sersecoshop.com**
Total Risk: **210**	Start Time: **14:52:14**	Finish Time: **16:44:53**
TCP/IP Fingerprint OS Estimate: **Linux**		

SecurityMetrics has determined that Serseco International, LLC. is NOT COMPLIANT with the PCI scan validation 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
Find public information regarding this IP, which an attacker could use to gain access: IP Information

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.

Port Scan

Protocol	Port	Program	Status	Summary	Turn 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.	HowTo
TCP	21	ProFTPD 1.3.0	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.	HowTo
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.	
		qmail		Your computer is running SMTP (Simple Mail Transport Protocol). This can be a security risk since a hacker can verify	

TCP	25	smtpd	Open	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.	HowTo
TCP	53	ISC BIND 9.3.4	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.	HowTo
UDP	53	ISC BIND 9.3.4	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.	HowTo
TCP	80	Apache httpd 2.2.2	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.	HowTo
TCP	106	poppassd	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.	HowTo
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.	HowTo
UDP	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.	HowTo
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.	HowTo
TCP	443	Apache httpd 2.2.2	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	qmail smtpd	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.	
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.	
TCP	3306	MySQL 5.0.27	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	8443	Apache httpd	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	8880	Apache httpd	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.	
UDP	32768	filenet-tms	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	52588		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.	

Security Vulnerabilities Solution Plan
The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in red and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in red but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. PCI Risk Table

Security Vulnerabilities

Protocol	Port	Program	Risk	Summary
TCP	443	https	8	Synopsis : The remote version of Apache is vulnerable to an off-by-one buffer overflow attack. Description : The remote host appears to be running a version of Apache which is older than 2.2.3. This version is vulnerable to an off-by-one buffer overflow attack in the mod_rewrite module. See also : http://www.apache.org/dist/httpd/Announc ement.html **Solution**: Upgrade to version 2.2.3. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-3747 BID : 19204 Other references : OSVDB:27588
TCP	443	https	8	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 5.2.4. Such versions may be affected by various issues, including but not limited to several overflows. See also : http://www.php.net/releases/5_2_4.php **Solution**: Upgrade to PHP version 5.2.4 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-2872, CVE-2007-3378, CVE-2007-3806 BID : 24661, 24261, 24922, 25498 Other references : OSVDB:36083, OSVDB:36085, OSVDB:36869
TCP	443	https	8	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 5.2.7. Such versions may be affected by several security issues : - File truncation can occur when calling 'dba_replace()' with an invalid argument. - There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371) - A buffer overflow in the 'imageloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658) - There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659) - When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg, 'file..php'). (CVE-2008-3660) - Multiple directory traversal vulnerabilities in functions such as 'posix_access()', 'chdir()', 'ftok()' may allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666). - A buffer overflow may be triggered when processing long message headers in 'php_imap.c' due to use of an obsolete API call. (CVE-2008-2829) - A heap-based buffer overflow may be triggered via a call to 'mb_check_encoding()', part of the 'mbstring' extension. (CVE-2008-5557) - Missing initialization of 'BG(page_uid)' and 'BG(page_gid)' when PHP is used as an Apache module may allow for bypassing security restriction due to SAPI 'php_getuid()' overloading. (CVE-2008-5624) - Incorrect 'php_value' order for Apache configuration may allow bypassing PHP's 'safe_mode' setting. (CVE-2008-5625) - The ZipArchive:extractTo() method in the ZipArchive extension fails to filter directory traversal sequences from file names. (CVE-2008-5658) See also : http://securityreason.com/achievement_se curityalert/57 http://securityreason.com/achievement_se curityalert/58 http://securityreason.com/achievement_se curityalert/59 http://www.sektioneins.de/advisories/SE- 2008-06.txt http://archives.neohapsis.com/archives/f ulldisclosure/2008-06/0238.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-06/0239.html http://www.openwall.com/lists/oss-securi ty/2008/08/08/2 http://www.openwall.com/lists/oss-securi ty/2008/08/13/8 http://archives.neohapsis.com/archives/f ulldisclosure/2008-11/0433.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-12/0089.html http://bugs.php.net/bug.php?id=42862 http://bugs.php.net/bug.php?id=45151 http://bugs.php.net/bug.php?id=45722 http://www.php.net/releases/5_2_7.php http://www.php.net/ChageLog-5.php#5.2.7 **Solution**: Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on. **Risk Factor**: High / CVSS Base Score : 7.5

				(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658 BID : 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948 Other references : OSVDB:46584, OSVDB:46638, OSVDB:46639, OSVDB:46641, OSVDB:46690, OSVDB:47796, OSVDB:47797, OSVDB:47798, OSVDB:50480, OSVDB:51477, OSVDB:52205, OSVDB:52206, OSVDB:52207
TCP	443	https	8	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 5.2.6. Such versions may be affected by the following issues : - A stack buffer overflow in FastCGI SAPI. - An integer overflow in printf(). - An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c. - A safe_mode bypass in cURL. - Incomplete handling of multibyte chars inside escapeshellcmd(). - Issues in the bundled PCRE fixed by version 7.6. See also : http://archives.neohapsis.com/archives/b ugtraq/2008-03/0321.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-05/0103.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-05/0107.html http://www.php.net/releases/5_2_6.php **Solution**: Upgrade to PHP version 5.2.6 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-4850, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051 BID : 27413, 28392, 29009 Other references : OSVDB:43219, OSVDB:44057, OSVDB:44906, OSVDB:44907, OSVDB:44908, Secunia:30048
TCP	443	https	8	Synopsis : The remote web server uses a version of PHP that is affected by multiple buffer overflows. Description : According to its banner, the version of PHP installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows. To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server, or to be able to manipulate several variables processed by some PHP functions such as htmlentities(). See also : http://www.php.net/releases/5_2_0.php **Solution**: Upgrade to PHP version 5.2.0 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-5465 BID : 20879 Other references : OSVDB:30178, OSVDB:30179
TCP	443	https	8	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 5.2.1. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals. See also : http://www.php.net/releases/5_2_1.php **Solution**: Upgrade to PHP version 5.2.1 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-1376, CVE-2007-1380, CVE-2007-1453, CVE-2007-1700, CVE-2007-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1890 BID : 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238 Other references : OSVDB:32776, OSVDB:32781, OSVDB:33955, OSVDB:34767
TCP	443	https	8	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 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows. See also : http://www.php.net/releases/5_2_5.php **Solution**: Upgrade to PHP version 5.2.5 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-4887, CVE-2007-5898, CVE-2007-5900 BID : 26403 Other references : OSVDB:38680, OSVDB:38681, OSVDB:38682, OSVDB:38683, OSVDB:38684, OSVDB:38685
				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 5.2.1. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals. See also :

TCP	80	http	8	http://www.php.net/releases/5_2_1.php **Solution**: Upgrade to PHP version 5.2.1 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-1376, CVE-2007-1380, CVE-2007-1453, CVE-2007-1700, CVE-2007-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1890 BID : 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238 Other references : OSVDB:32776, OSVDB:32781, OSVDB:33955, OSVDB:34767
TCP	80	http	8	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 5.2.6. Such versions may be affected by the following issues : - A stack buffer overflow in FastCGI SAPI. - An integer overflow in printf(). - An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c. - A safe_mode bypass in cURL. - Incomplete handling of multibyte chars inside escapeshellcmd(). - Issues in the bundled PCRE fixed by version 7.6. See also : http://archives.neohapsis.com/archives/b ugtraq/2008-03/0321.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-05/0103.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-05/0107.html http://www.php.net/releases/5_2_6.php **Solution**: Upgrade to PHP version 5.2.6 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-4850, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051 BID : 27413, 28392, 29009 Other references : OSVDB:43219, OSVDB:44057, OSVDB:44906, OSVDB:44907, OSVDB:44908, Secunia:30048
TCP	80	http	8	Synopsis : The remote version of Apache is vulnerable to an off-by-one buffer overflow attack. Description : The remote host appears to be running a version of Apache which is older than 2.2.3. This version is vulnerable to an off-by-one buffer overflow attack in the mod_rewrite module. See also : http://www.apache.org/dist/httpd/Announc ement.html **Solution**: Upgrade to version 2.2.3. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-3747 BID : 19204 Other references : OSVDB:27588
TCP	80	http	8	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 5.2.7. Such versions may be affected by several security issues : - File truncation can occur when calling 'dba_replace()' with an invalid argument. - There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371) - A buffer overflow in the 'imageloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658) - There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659) - When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg, 'file..php'). (CVE-2008-3660) - Multiple directory traversal vulnerabilities in functions such as 'posix_access()', 'chdir()', 'ftok()' may allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666). - A buffer overflow may be triggered when processing long message headers in 'php_imap.c' due to use of an obsolete API call. (CVE-2008-2829) - A heap-based buffer overflow may be triggered via a call to 'mb_check_encoding()', part of the 'mbstring' extension. (CVE-2008-5557) - Missing initialization of 'BG(page_uid)' and 'BG(page_gid)' when PHP is used as an Apache module may allow for bypassing security restriction due to SAPI 'php_getuid()' overloading. (CVE-2008-5624) - Incorrect 'php_value' order for Apache configuration may allow bypassing PHP's 'safe_mode' setting. (CVE-2008-5625) - The ZipArchive:extractTo() method in the ZipArchive extension fails to filter directory traversal sequences from file names. (CVE-2008-5658) See also : http://securityreason.com/achievement_se curityalert/57 http://securityreason.com/achievement_se curityalert/58 http://securityreason.com/achievement_se curityalert/59 http://www.sektioneins.de/advisories/SE- 2008-06.txt http://archives.neohapsis.com/archives/f ulldisclosure/2008-06/0238.html http://archives.neohapsis.com/archives/f ulldisclosure/2008-06/0239.html http://www.openwall.com/lists/oss-securi ty/2008/08/08/2 http://www.openwall.com/lists/oss-securi ty/2008/08/13/8 http://archives.neohapsis.com/archives/f ulldisclosure/2008-11/0433.html

				http://archives.neohapsis.com/archives/f ulldisclosure/2008-12/0089.html http://bugs.php.net/bug.php?id=42862 http://bugs.php.net/bug.php?id=45151 http://bugs.php.net/bug.php?id=45722 http://www.php.net/releases/5_2_7.php http://www.php.net/ChageLog-5.php#5.2.7 **Solution**: Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658 BID : 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948 Other references : OSVDB:46584, OSVDB:46638, OSVDB:46639, OSVDB:46641, OSVDB:46690, OSVDB:47796, OSVDB:47797, OSVDB:47798, OSVDB:50480, OSVDB:51477, OSVDB:52205, OSVDB:52206, OSVDB:52207
TCP	80	http	**8**	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 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows. See also : http://www.php.net/releases/5_2_5.php **Solution**: Upgrade to PHP version 5.2.5 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-4887, CVE-2007-5898, CVE-2007-5900 BID : 26403 Other references : OSVDB:38680, OSVDB:38681, OSVDB:38682, OSVDB:38683, OSVDB:38684, OSVDB:38685
TCP	80	http	**8**	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 5.2.4. Such versions may be affected by various issues, including but not limited to several overflows. See also : http://www.php.net/releases/5_2_4.php **Solution**: Upgrade to PHP version 5.2.4 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2007-2872, CVE-2007-3378, CVE-2007-3806 BID : 24661, 24261, 24922, 25498 Other references : OSVDB:36083, OSVDB:36085, OSVDB:36869
TCP	80	http	**8**	Synopsis : The remote web server uses a version of PHP that is affected by multiple buffer overflows. Description : According to its banner, the version of PHP installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows. To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server, or to be able to manipulate several variables processed by some PHP functions such as htmlentities(). See also : http://www.php.net/releases/5_2_0.php **Solution**: Upgrade to PHP version 5.2.0 or later. **Risk Factor**: High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE : CVE-2006-5465 BID : 20879 Other references : OSVDB:30178, OSVDB:30179
TCP	443	https	**7**	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 5.2.3. Such versions may be affected by several issues, including an integer overflow, 'safe_mode' and 'open_basedir' bypass, and a denial of service vulnerability. See also : http://www.php.net/releases/5_2_3.php **Solution**: Upgrade to PHP version 5.2.3 or later. **Risk Factor**: Medium / CVSS Base Score : 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) CVE : CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007 BID : 23359, 24089, 24259, 24261 Other references : OSVDB:33962, OSVDB:35788, OSVDB:36083, OSVDB:36084, OSVDB:36643
TCP	80	http	**7**	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 5.2.3. Such versions may be affected by several issues, including an integer overflow, 'safe_mode' and 'open_basedir' bypass, and a denial of service vulnerability. See also : http://www.php.net/releases/5_2_3.php **Solution**: Upgrade to PHP version 5.2.3 or later. **Risk Factor**: Medium / CVSS Base Score : 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) CVE : CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007 BID : 23359, 24089, 24259, 24261 Other references : OSVDB:33962, OSVDB:35788, OSVDB:36083, OSVDB:36084, OSVDB:36643

TCP	8443	pcsync-https	**7**	We detected a vulnerable version of the DCShop CGI. This version does not properly protect user and credit card information. It is possible to access files that contain administrative passwords, current and pending transactions and credit card information (along with name, address, etc). The following files are affected: DCShop orders file: /styles/Orders/orders.txt DCShop orders file: /styles/orders/orders.txt DCShop authentication file: /styles/Auth_data/auth_user_file.txt DCShop authentication file: /styles/auth_data/auth_user_file.txt **Solution**: 1. Rename following directories to something hard to guess: - Data - User_carts - Orders - Auth_data 2. Make these changes to dcshop.setup and dcshop_admin.setup. - In dcshop.setup, modify: $datadir = '$cgidir/Data' $cart_dir = '$cgidir/User_carts' $order_dir = '$cgidir/Orders' - In dcshop_admin.setup, modify: $password_file_dir = '$path/Auth_data' 3. Rename dcshop.setup and dcshop_admin.setup to something difficult to guess. For example, dcshop_4314312.setup and dcshop_admin_3124214.setup 4. Edit dcshop.cgi, dcshop_admin.cgi, and dcshop_checkout.cgi and modify the require statement for dcshop.setup and dcshop_admin.setup. That is: - In dcshop.cgi, modify require '$path/dcshop.setup' so that it uses new setup file. For example, require '$path/dcshop_4314312.setup' - In dcshop_admin.cgi, modify require '$path/dcshop.setup' require '$path/dcshop_admin.setup' so that it uses new setup file. For example, require '$path/dcshop_4314312.setup' require '$path/dcshop_admin_3124214.setup' - In dcshop_checkout.cgi, modify require '$path/dcshop.setup' so that it uses new setup file. For example, require '$path/dcshop_4314312.setup' 5. Save following file as index.html and upload it to your /cgi-bin/dcshop directory, thereby hiding directory listing. On NT servers, you may have to rename this file to default.htm. http://www.dcscripts.com/FAQ/ This page show 'Internal Server Error' so it is not an error page... it's just an index.html file to HIDE directories. 6. Replace your current files with above files **Risk Factor**: High Additional information: http://www.securiteam.com/unixfocus/5RP0_N2K4KE.html CVE : CAN-2001-0821 BID : 2889
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-mirr or/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-2 4 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 /SMetrics196317510.html HTTP/1.1 Connection: Close Host: www.sersecoshop.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: Wed, 19 Aug 2009 20:40:44 GMT Server: Apache/2.2.2 (Fedora) Connection: close Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics196317510.html HTTP/1.1 Connection: Close Host: www.sersecoshop.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

Synopsis : The remote web server may be affected by several issues.

TCP	443	https	5	Description : According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including : - Improper handling of excessive forwarded interim responses may cause denial-of-service conditions in mod_proxy_http. (CVE-2008-2364) - A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420) - The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195) Note that the remote web server may not actually be affected by these vulnerabilities. SMetrics did not try to determine whether the affected modules are in use or to check for the issues themselves. See also : https://bugzilla.redhat.com/show_bug.cgi ?id=489436 http://www.apache.org/dist/httpd/CHANGES_2.2 http://httpd.apache.org/security/vulnera bilities_22.html **Solution**: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 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-2007-6420, CVE-2008-2364, CVE-2009-1195 BID : 27236, 29653, 35115 Other references : OSVDB:42937, OSVDB:46085, OSVDB:54733, Secunia:30621
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 : 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
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/downlo ads/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)
				Synopsis : The remote web server might transmit credentials in cleartext. Description : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid

TCP	80	http	**5**	users. **Solution**: Make sure that every sensitive form transmits content over HTTPS. **Risk Factor**: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : Page : / Destination page : sis/wib/aplic/login.php?8kYaT8mNVklw Input name : password Page : /Home.htm Destination page : sis/wib/aplic/login.php?T8l6FnACbxTi Input name : password Page : /. Destination page : sis/wib/aplic/login.php?gCmodU2f1d9a Input name : password Page : /index.htm Destination page : sis/wib/aplic/login.php?e4cDqw5U4SFZ Input name : password Page : /Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?PKiHFP2keOWc Input name : password Page : /Recomendados.htm Destination page : sis/wib/aplic/login.php?tr6paGxvThvO Input name : password Page : /faq.htm Destination page : sis/wib/aplic/login.php?M6Gu5yKsJ1D6 Input name : password Page : /Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?eY3L2b97pnG1 Input name : password Page : /contactenos.htm Destination page : sis/wib/aplic/login.php?CfDzxL7KAHV2 Input name : password Page : /contra.htm Destination page : sis/wib/aplic/login.php?tTs7PR1fWjgE Input name : password Page : /registro.htm Destination page : sis/wib/aplic/login.php?GhUUZAXwx7tn Input name : password Page : /detalle_noticia.htm Destination page : sis/wib/aplic/login.php?APieDVMHDsZn Input name : password Page : /Mapa_del_Sitio.htm Destination page : sis/wib/aplic/login.php?vS1h6xFryI1P Input name : password Page : /Noticias.htm Destination page : sis/wib/aplic/login.php?qgU25cmc4uX7 Input name : password Page : /Terminos_y_Condiciones_de_Uso.htm Destination page : sis/wib/aplic/login.php?xwFKakWbnUSp Input name : password Page : /ABOUT_US.htm Destination page : sis/wib/aplic/login.php?jYOqw4SfmPLD Input name : password Page : /Products.htm Destination page : sis/wib/aplic/login.php?VWfp4FctesbG Input name : password Page : /FAQeng.htm Destination page : sis/wib/aplic/login.php?hzoS4DJsO2DV Input name : password Page : /BUY.htm Destination page : sis/wib/aplic/login.php?rn2Y51HIv9fg Input name : password Page : /CONTACT_US.htm Destination page : sis/wib/aplic/login.php?beWoUs0m9r1F Input name : password Page : /Forgot_Password.htm Destination page : sis/wib/aplic/login.php?z1TOvjgiurrG Input name : password Page : /Sign_Up.htm Destination page : sis/wib/aplic/login.php?9peiaQtW0GLj Input name : password Page : /News.htm Destination page : sis/wib/aplic/login.php?rvp22fQ3lSlG Input name : password Page : /./Home.htm Destination page : sis/wib/aplic/login.php?ooX14Lb9HETP Input name : password Page : /./Products.htm Destination page : sis/wib/aplic/login.php?1trbbkxHJaug Input name : password Page : /./FAQeng.htm Destination page : sis/wib/aplic/login.php?Xn3hUnDXRI2E Input name : password Page : /./BUY.htm Destination page : sis/wib/aplic/login.php?HqdsOYaAS4RJ Input name : password Page : /./CONTACT_US.htm Destination page : sis/wib/aplic/login.php?uKsVVHN2BfEm Input name : password Page : /./Site_Map.htm Destination page : sis/wib/aplic/login.php?4RwIb0hvngka Input name : password Page : /./News.htm Destination page : sis/wib/aplic/login.php?B89jGHebd9GY Input name : password Page : /./Terms_and_Conditions.htm Destination page : sis/wib/aplic/login.php?gcbpBMlr3dEj Input name : password Page : /./index.htm Destination page : sis/wib/aplic/login.php?2FDK1QgWFBtg Input name : password Page : /./ABOUT_US.htm Destination page : sis/wib/aplic/login.php?9cS8RraaxAV7 Input name : password Page : /./Forgot_Password.htm Destination page : sis/wib/aplic/login.php?RsD6Lwr6FjeB Input name : password Page : /./Sign_Up.htm Destination page : sis/wib/aplic/login.php?V9ypgj3UW8fx Input name : password Page : /./detalle_noticia.htm Destination page : sis/wib/aplic/login.php?DVK70aUNDTFC Input name : password Page : /./Quienes_Somos.htm Destination page : sis/wib/aplic/login.php?H61xYZ9W7EFt Input name : password Page : /./Recomendados.htm Destination page : sis/wib/aplic/login.php?OgCgv7wQ7wNu Input name : password Page : /./faq.htm Destination page : sis/wib/aplic/login.php?1BJKn10PwmGo Input name : password Page : /./Hacer_una_Compra.htm Destination page : sis/wib/aplic/login.php?XKQcpxI0MmuI Input name : password Page : /./contactenos.htm Destination page : sis/wib/aplic/login.php?deq2Y2vz2sff Input name : password Page : /./contra.htm Destination page : sis/wib/aplic/login.php?UgLFiLOpYWB2 Input name : password Page : /./registro.htm Destination page : sis/wib/aplic/login.php?CgigbBjHyfct Input name : password Page : /./Mapa_del_Sitio.htm

TCP	80	http	5	Destination page : sis/wib/aplic/login.php?mYFz234odrRS Input name : password Page : /./Noticias.htm Destination page : sis/wib/aplic/login.php?Lu7yqOZP2ygH Input name : password
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-mirr or/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-2 4 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 /SMetrics473767439.html HTTP/1.1 Connection: Close Host: www.sersecoshop.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: Wed, 19 Aug 2009 20:40:44 GMT Server: Apache/2.2.2 (Fedora) Connection: close Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics473767439.html HTTP/1.1 Connection: Close Host: www.sersecoshop.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	80	http	5	Synopsis : The remote web server may be affected by several issues. Description : According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including : - Improper handling of excessive forwarded interim responses may cause denial-of-service conditions in mod_proxy_http. (CVE-2008-2364) - A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420) - The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195) Note that the remote web server may not actually be affected by these vulnerabilities. SMetrics did not try to determine whether the affected modules are in use or to check for the issues themselves. See also : https://bugzilla.redhat.com/show_bug.cgi ?id=489436 http://www.apache.org/dist/httpd/CHANGES_2.2 http://httpd.apache.org/security/vulnera bilities_22.html **Solution**: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 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-2007-6420, CVE-2008-2364, CVE-2009-1195 BID : 27236, 29653, 35115 Other references : OSVDB:42937, OSVDB:46085, OSVDB:54733, Secunia:30621
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 : 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	8443	pcsync-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-mirr or/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-2 4 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 /SMetrics2066351228.html HTTP/1.1 Connection: Close Host: www.sersecoshop.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: Wed, 19 Aug 2009 20:40:44 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: message/http TRACE /SMetrics2066351228.html HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Charset: iso-8859-1,*,utf-8 Accept-Language: en Connection: Close Host: www.sersecoshop.com Pragma: no-cache User-Agent: Mozilla/4.75 [en] (X11, U Smetrics) ---------- snip ---------- CVE : CVE-2003-1567, CVE-2004-2320 BID : 9506, 9561, 11604, 33374 Other references : OSVDB:877, OSVDB:3726, OSVDB:5648
TCP		http/https	4	Possible cross site scripting on http://sersecoshop.com/sis/wib/aplic/07mostrarfoto.php Use the following commands to verify this: wp --inject "http://sersecoshop.com/sis/wib/aplic/07_mostrarfoto.php?Descripcion=%3Cscript%3Eal ert%28%22XSS%22%29%3B%3C%2Fscript%3E&Image n=" POST curl -L -d "Descripcion=%3Cscript%3Ealert%28%22XSS%2 2%29%3B%3C%2Fscript%3E&Imagen=" "http://sersecoshop.com/sis/wib/aplic/07_mostrarfoto.php"| grep "XSS" This website may have other injection related vulnerabilities.
TCP	80	http	4	Synopsis : The remote web server is prone to cross-site scripting attacks. Description : The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. See also : http://en.wikipedia.org/wiki/Cross-site_scripting

				Solution: Contact the vendor for a patch or upgrade. **Risk Factor**: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) CVE : CVE-2002-1060, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681 BID : 5305, 7344, 7353, 8037, 14473, 17408 Other references : OSVDB:4989, OSVDB:18525, OSVDB:24469, OSVDB:42314
TCP	8443	pcsync-https	4	'shopadmin.asp' is installed. Some versions of this script are vulnerable to SQL injection. **Solution**: Move to a different directory or use a different shopping cart. From VP-ASP 3.0 and higher set the following in shop\$config.asp const xAdminPage=youradminpagename.asp const xShowAdmin=No bugtraq id: 4861 **Risk Factor**: Medium BID : 4861
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 web server may be affected by several issues. Description : According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including : - A cross-site scripting issue involving mod_imagemap (CVE-2007-5000). - A cross-site scripting issue involving 413 error pages via a malformed HTTP method (PR 44014 / CVE-2007-6203). - A cross-site scripting issue in mod_status involving the refresh parameter (CVE-2007-6388). - A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421). - A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422). - A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset (CVE-2008-0005). Note that the remote web server may not actually be affected by these vulnerabilities. SMetrics did not try to determine whether the affected modules are in use or to check for the issues themselves. See also : http://www.apache.org/dist/httpd/CHANGES_2.2 http://httpd.apache.org/security/vulnera bilities_22.html **Solution**: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P) CVE : CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005 BID : 26663, 26838, 27234, 27236, 27237 Other references : OSVDB:39003, OSVDB:39134, OSVDB:40262, OSVDB:40263, OSVDB:40264, OSVDB:42214, OSVDB:42937
TCP	80	http	3	Synopsis : The remote web server may be affected by several issues. Description : According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including : - A cross-site scripting issue involving mod_imagemap (CVE-2007-5000). - A cross-site scripting issue involving 413 error pages via a malformed HTTP method (PR 44014 / CVE-2007-6203). - A cross-site scripting issue in mod_status involving the refresh parameter (CVE-2007-6388). - A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421). - A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422). - A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset (CVE-2008-0005). Note that the remote web server may not actually be affected by these vulnerabilities. SMetrics did not try to determine whether the affected modules are in use or to check for the issues themselves. See also : http://www.apache.org/dist/httpd/CHANGES_2.2 http://httpd.apache.org/security/vulnera bilities_22.html **Solution**: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later. **Risk Factor**: Low / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P) CVE : CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005 BID : 26663, 26838, 27234, 27236, 27237 Other references : OSVDB:39003, OSVDB:39134, OSVDB:40262, OSVDB:40263,

				OSVDB:40264, OSVDB:42214, OSVDB:42937
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	The following IP protocols are accepted on this host: 1 ICMP 2 IGMP 6 TCP 17 UDP 136 UDPLite
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
UDP		general/udp	0	For your information, here is the traceroute from 204.238.82.18 to 69.94.134.202 : 204.238.82.18 204.238.82.2 64.90.192.39 206.71.65.41 64.78.227.85 64.78.230.202 4.71.40.1 4.68.107.62 4.69.132.37 4.69.132.106 4.69.145.76 4.68.111.174 152.63.96.86 152.63.10.114 152.63.51.117 157.130.213.110 69.94.134.202
TCP		general/tcp	0	69.94.134.202 resolves as www.sersecoshop.com.
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
UDP	111	sunrpc	0	Synopsis : An ONC RPC service is running on the remote host. Description : By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port. **Risk Factor**: None
TCP	111	sunrpc	0	Synopsis : An ONC RPC portmapper is running on the remote host. Description : The RPC portmapper is running on this port. The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request. **Risk Factor**: None
TCP	111	sunrpc	0	Synopsis : An ONC RPC service is running on the remote host. Description : By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port. **Risk Factor**: None
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	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 1998-2004 Double Precision, Inc. See COPYING for distribution information.
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	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. **Risk Factor**: None
TCP	22	ssh	0	Synopsis : An SSH server is running on the remote host. Description : This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. **Risk Factor**: None Plugin output : The remote SSH

				daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : 98:61:94:53:2c:4a:77:13:a6:d6:3a:a2:b4:6e :eb:fe
TCP	22	ssh	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	25	smtp	0	A SMTP server is running on this port
TCP	25	smtp	0	For some reason, we could not send the EICAR test string to this MTA.
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
UDP	32768	filenet-tms	0	Synopsis : An ONC RPC service is running on the remote host. Description : By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port. **Risk Factor**: None
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. It is possible to extract the version number of the remote installation from the server greeting. **Solution**: Restrict access to the database to allowed IPs only. **Risk Factor**: None Plugin output : The remote MySQL version is 5.0.27
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/2.2.2 (Fedora) **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 : 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	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	465	urd	0	A SMTP server is running on this port
TCP	465	urd	0	For some reason, we could not send the EICAR test string to this MTA.
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
				Synopsis : An ONC RPC service is running on the remote host. Description : By sending a DUMP request to the portmapper, it was possible to

TCP	52588	unknown	0	enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote 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 : 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
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=5 713 **Solution**: Restrict access to your DNS server from public network or reconfigure it to reject such queries. **Risk Factor**: None
UDP	53	domain	0	Synopsis : The remote domain publishes SPF records. Description : The remote domain publishes SPF records. SPF (Sender Policy Framework) is a mechanism to let an organization specify their mail sending policy, such as which mail servers are authorized to send mail on its behalf. See also : http://www.openspf.org/ **Risk Factor**: None
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. **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
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 : 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 : 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/2.2.2 (Fedora) **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 : 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	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: /_backup, /cgi-bin, /pipermail, /test, /css, /error, /icons, /image, /images, /img, /mailman, /manual, /styles 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 Other references : OWASP:OWASP-CM-006
TCP	8443	pcsync-https	0	A web server is running on this port
TCP	8443	pcsync-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	8443	pcsync-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 and the 'ServerTokens' directive is ProductOnly Apache does not offer a way to hide the server type.
TCP	8443	pcsync-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	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	A POP3 server is running on this port
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

For a list of all vulnerabilities in our knowledge base on this test date click here.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-04, within the guidelines of the PCI data security initiative.