

securityMETRICS®

ASV Scan Report Vulnerability Details

The Digital Ranch, Inc.

Scan Results Table of Contents

Domain/IP	Max Risk	Domain/IP	Max Risk
<hr/>			

Test Results

Executive Summary		
Test Result: Pass	Date: 2011-12-02	Target IP: www.everythingcu.com
Test ID: 3397977	Test Length: 49.65 Minutes	DNS Entry: No Reverse DNS Reply
Total Risk: 8	Start Time: 17:21:38	Finish Time: 18:11:17
TCP/IP Fingerprint OS Estimate: Microsoft Windows		Scan Expiration: 2012-03-01

Congratulations, the computer **passes** because no risk of 4 or more was found.

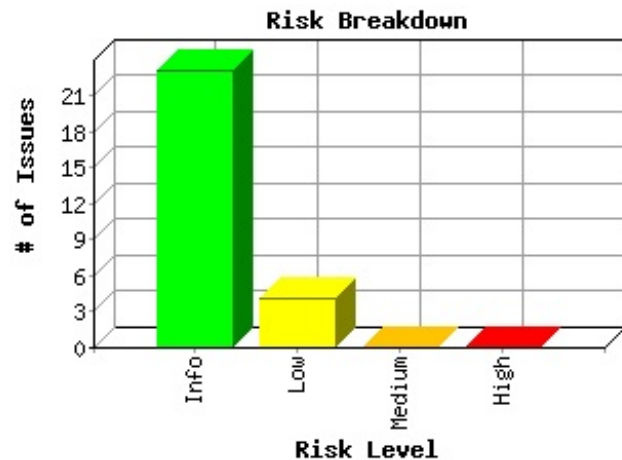
Attackers typically use footprinting, port scanning and security vulnerability testing to find security weaknesses on computers. This report provides information on each of these categories.

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.	
TCP	80	Microsoft IIS webserver 6.0	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	Microsoft IIS webserver 6.0	Open	Your computer appears to be running HTTP Secure Socket Layer (SSL) software. This software improves the security of HTTP communication with this server.	

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	80	http	3	Synopsis : The remote web server is running Microsoft IIS. Description : The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk. Note that this test makes assumptions of the remote patch level based on static return values (Content-Length) within a IIS Server's 404 error message. As such, the test can not be totally reliable and should be manually confirmed. Note also that, to determine IIS6 patch levels, a simple test is done based on strict RFC 2616 compliance. It appears as if IIS6-SP1 will accept CR as an end-of-line marker instead of both CR and LF. Solution: Ensure that the server is running the latest stable Service Pack. Risk Factor: None Plugin output : The remote IIS server *seems* to be Microsoft IIS 6.0 - SP1
TCP	80	http	3	Synopsis : The remote web server generates predictable session IDs. Description : The remote web server generates a session ID for each connection. A session ID is typically used to keep track of the actions of a user while he visits a web site. The remote server generates non-random session IDs. An attacker might use this flaw to guess the session IDs of other users and therefore steal their session. See also : http://pdos.csail.mit.edu/cookies/seq_sessionid.html Solution: Configure the remote site and CGIs so as to use random session IDs. Risk Factor: Medium / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
TCP	443	https	1	The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages. Specifically, the following methods are enabled on the remote webserver: - IIS NTLM

				authentication is enabled Solution: None at this time Risk Factor: Low CVE : CVE-2002-0419 BID : 4235
TCP	80	http	1	The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages. Specifically, the following methods are enabled on the remote webserver: - IIS NTLM authentication is enabled Solution: None at this time Risk Factor: Low CVE : CVE-2002-0419 BID : 4235
UDP		general/udp	0	For your information, here is the traceroute from x.x.x.x55 to 204.246.144.9 : x.x.x.x55 x.x.x.x 204.238.82.2 66.51.1.54 66.51.1.61 66.51.1.42 66.51.1.98 204.246.144.9
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 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		general/tcp	0	Remote operating system : Microsoft Windows Server 2003 Confidence Level : 75 Method : HTTP The remote host is running Microsoft Windows Server 2003
TCP		general/tcp	0	204.246.144.9 resolves as www.everythingcu.com.
TCP		general/tcp	0	The TCP sequence numbers may be constant; An attacker may use this flaw to spoof TCP connections easily. Solution: contact your vendor for a patch
TCP		general/tcp	0	the IP ID sequence generation is: Randomized
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 : Microsoft-IIS/6.0
TCP	443	https	0	Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robots.txt.org/wc/exclusion.html Solution: Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material. Risk Factor: None Contents of robots.txt : User-agent: * Disallow: /automatedtasks/ Disallow: /beehive/ Disallow: /beehivedemo/ Disallow: /beta/ Disallow: /bookstore/ Disallow: /campaigns/ Disallow: /careercenter/ Disallow: /cfcs/ Disallow: /cfcustomtags/ Disallow: /ckeditor/ Disallow: /eagle/ Disallow: /files/ Disallow: /fiscal/ Disallow: /functions/ Disallow: /henricoprototype/ Disallow: /jobtracking/ Disallow: /launchcodes/ Disallow: /marketingreport/ Disallow: /queries/ Disallow: /services/productactionfiles/ Disallow: /switchkit/ Disallow: /switchkit_old/ Disallow: /switchkitprem/ Disallow: /tablecreate/ Disallow: /test/ Disallow: /test_connection/ Disallow: /testimonials/ Disallow: /whiteriver/ Disallow: /XYZNWSK/ Disallow: /application.cfm Disallow: /dsp_searchresults2.cfm Other references : OSVDB:238
TCP	443	https	0	A TLSv1 server answered on this port
TCP	443	https	0	A web server is running on this port through SSL
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
				Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 29:b2:6a:8e:69:a9:19:c1:ab:da:27:a9:40:c1:b6:87 Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Thawte, Inc., CN=Thawte SSL CA Validity Not Before: Feb 2 00:00:00 2011 GMT Not After : Mar 3 23:59:59 2013 GMT Subject: C=US, ST=Massachusetts, L=Holyoke, O=Partee Creative Inc., CN=www.everythingcu.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:bf:eb:c0:6a:bc:98:67:a1:63:2a:90:c9:7d:41: 92:4d:af:dd:9a:10:43:cc:47:88:72:f5:97:2b:64: 22:aa:66:83:54:48:0e:55:1c:c4:5c:4c:0b:8b:d0: 8c:6e:14:20:fa:a2:bf:a3:90:91:c6:c5:cb:96:5a: bd:70:37:44:a1:8e:c3:59:92:a1:c5:f8:df:f1:d7: 5d:65:02:e8:d4:a3:5b:a4:3a:a8:41:04:58:7e:68: 64:84:4f:66:42:14:c7:37:5a:34:c8:1e:72:8c:17: 0f:fd:9e:0f:67:8b:56:59:77:29:34:ef:02:08:fa: 64:02:14:4a:dd:57:48:c4:02:4a:6c:f5:9c:ea:58: 0e:7e:0a:0d:de:f6:3a:6f:f7:db:53:ff:10:24:54: fe:32:1a:30:1f:c8:2b:80:4a:95:bf:a0:ff:a9:77: dc:fa:b2:1a:3c:8d:1a:bb:2a:8a:46:95:26:18:ac:

TCP	443	https	0	93:c1:37:e9:e3:6a:e9:7b:7f:47:48:7a:e5:b8:7c:be:63:7a:6e:be:6c:98:db:62:f0:c3:40:c1:7f:03:0d:ed:36:20:9e:bd:09:bc:c6:35:c2:d5:aa:a8:2c:be:c4:14:b6:51:12:61:5e:35:f6:d9:b2:1e:44:cb:57:21:9b:e7:61:7d:41:dc:0c:77:47:5a:d2:96:2b:d1:fb Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: critical CA:FALSE X509v3 CRL Distribution Points: URI: http://svr-ov-crl.thawte.com/ThawteO.V.crl X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication Authority Information Access: OCSP - URI: http://ocsp.thawte.com Signature Algorithm: sha1WithRSAEncryption 89:44:b3:7f:65:84:78:9b:48:80:f9:cb:f8:89:d4:a5:07:5e:28:f9:a1:3f:f1:48:37:66:33:b8:0d:bf:58:8b:e3:f7:7e:43:52:28:a5:b4:23:7e:cd:23:6b:63:fa:c2:94:b4:56:34:34:a9:a7:17:8a:ae:b7:52:ae:f4:59:65:03:09:e8:bb:36:5a:a4:97:c5:50:48:46:8f:53:db:c2:e4:15:75:52:49:2b:20:a4:24:56:b0:ab:6d:0a:4d:85:c8:4d:90:11:37:09:4a:a1:82:99:42:eb:c3:5f:5d:c1:30:42:ea:d5:0d:94:15:0a:3d:fc:c7:54:dd:3c:f8:17:65:0f:bc:71:55:59:db:bd:71:70:12:85:38:9e:c2:67:49:bb:e5:64:a8:2e:fd:15:cc:ed:da:eb:6d:08:53:1c:fb:19:e6:d8:e4:9d:ce:6f:b6:b8:74:fe:ed:a1:44:cb:6a:d2:49:a8:24:b3:83:20:ac:07:49:87:dc:02:42:54:68:e2:48:82:72:60:6d:2a:3d:9f:e7:47:40:dd:ee:ef:8f:b9:ae:f7:35:7a:e5:9d:c0:ff:51:eb:f5:7c:dd:ea:06:63:5b:fa:87:b9:ed:d9:97:64:4b:a9:56:48:5d:b1:7e:be:d5:34:c5:65:d2:f9:f8:5d:83:ac:9e:04:e4:e7 This TLSv1 server does not accept SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.
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: /cfide, /beta, /files, /images, /us, /automatedtasks, /beehive, /bookstore, /cfcs, /cfcustomtags, /ckeditor, /fiscal, /functions, /henricoprotype, /launchcodes, /queries, /services/productactionfiles, /switchkit, /switchkit_old, /switchkitprem, /tablecreate, /test_connection, /testimonials, /XYZNWSK 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 is running Microsoft IIS. Description : The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk. Note that this test makes assumptions of the remote patch level based on static return values (Content-Length) within a IIS Server's 404 error message. As such, the test can not be totally reliable and should be manually confirmed. Note also that, to determine IIS6 patch levels, a simple test is done based on strict RFC 2616 compliance. It appears as if IIS6-SP1 will accept CR as an end-of-line marker instead of both CR and LF. Solution: Ensure that the server is running the latest stable Service Pack. Risk Factor: None Plugin output : The remote IIS server *seems* to be Microsoft IIS 6.0 - SP1
TCP	443	https	0	Nmap has identified this service as Microsoft IIS webservice 6.0
TCP	443	https	0	Synopsis : The remote service encrypts communications using SSL. Description : This script detects which SSL ciphers are supported by the remote service for encrypting communications. See also : http://www.openssl.org/docs/apps/ciphers.html Risk Factor: None Plugin output : Here is the list of SSL ciphers supported by the remote server : High Strength Ciphers (>= 112-bit key) SSLv3 DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1 RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5 RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1 The fields above are : {OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}
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	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 : Microsoft-IIS/6.0
TCP	80	http	0	Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robots.txt.org/wc/exclusion.html Solution: Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material. Risk Factor: None Contents of robots.txt : User-agent: * Disallow: /automatedtasks/ Disallow: /beehive/ Disallow: /beehivedemo/ Disallow: /beta/ Disallow: /bookstore/ Disallow: /campaigns/ Disallow: /careercenter/

				Disallow: /cfcs/ Disallow: /cfcustomtags/ Disallow: /ckeditor/ Disallow: /eagle/ Disallow: /files/ Disallow: /fiscal/ Disallow: /functions/ Disallow: /henricoprototype/ Disallow: /jobtracking/ Disallow: /launchcodes/ Disallow: /marketingreport/ Disallow: /queries/ Disallow: /services/productactionfiles/ Disallow: /switchkit/ Disallow: /switchkit_old/ Disallow: /switchkitprem/ Disallow: /tablecreate/ Disallow: /test/ Disallow: /test_connection/ Disallow: /testimonials/ Disallow: /whiteriver/ Disallow: /XYZNWSK/ Disallow: /application.cfm Disallow: /dsp_searchresults2.cfm Other references : OSVDB:238
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: /cfide, /beta, /files, /images, /us, /automatedtasks, /beehive, /bookstore, /cfcs, /cfcustomtags, /ckeditor, /fiscal, /functions, /henricoprototype, /launchcodes, /queries, /services/productactionfiles, /switchkit, /switchkit_old, /switchkitprem, /tablecreate, /test_connection, /testimonials, /XYZNWSK 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	Nmap has identified this service as Microsoft IIS webserver 6.0
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

For a list of all vulnerabilities in our knowledge base on this test date [click here](#).

CONFIDENTIAL AND PROPRIETARY INFORMATION

SECURITYMETRICS PROVIDES THIS INFORMATION "AS IS" WITHOUT ANY WARRANTY OF ANY KIND. SECURITYMETRICS MAKES NO WARRANTY THAT THESE SERVICES WILL DETECT EVERY VULNERABILITY ON YOUR COMPUTER, OR THAT THE SUGGESTED SOLUTIONS AND ADVICE PROVIDED IN THIS REPORT, TOGETHER WITH THE RESULTS OF THE VULNERABILITY ASSESSMENT, WILL BE ERROR-FREE OR COMPLETE. SECURITYMETRICS SHALL NOT BE RESPONSIBLE OR LIABLE FOR THE ACCURACY, USEFULNESS, OR AVAILABILITY OF ANY INFORMATION TRANSMITTED VIA THE SECURITYMETRICS SERVICE, AND SHALL NOT BE RESPONSIBLE OR LIABLE FOR ANY USE OR APPLICATION OF THE INFORMATION CONTAINED IN THIS REPORT. DISSEMINATION, DISTRIBUTION, COPYING OR USE OF THIS DOCUMENT IN WHOLE OR IN PART BY A SECURITYMETRICS COMPETITOR OR THEIR AGENTS IS STRICTLY PROHIBITED.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-06, within the guidelines of the PCI data security initiative.