



New Report

Save Report

July 8, 2009

**1.0 Introduction**

SAINT has determined that customer is not globally PCI compliant with the PCI scan validation requirement. The scan was conducted on June 29, 2009, at 3:01 PM. A heavy vulnerability assessment was conducted using the SAINT® 7.0 vulnerability scanner. The scan discovered a total of five live hosts, and detected 42 critical problems, 94 areas of concern, and 110 potential problems. The hosts and problems detected are discussed in greater detail in the following sections. This report was generated by a PCI Approved Scanning Vendor, SAINT Corporation, under certificate number 4268-01-02, within the guidelines of the PCI data security initiative.

**2.0 Overview**

The following vulnerability severity levels are used to categorize the vulnerabilities:

**CRITICAL PROBLEMS**

Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

**AREAS OF CONCERN**

Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

**POTENTIAL PROBLEMS**

Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

**SERVICES**

Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

**2.1 Vulnerability List**

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	CVSSv2 Base Score	PCI Compliant?
host1.domain.com	critical	Download.Ject detected on web server	Other			no
host1.domain.com	critical	Guessed password to windows account (foobar:foobar)	Passwords			no
host1.domain.com	critical	MS FrontPage Server Extension Vulnerability: /_vti_bin/shtml.dll	Web	<a href="#">CVE-2003-0824</a>	5.0	no
host1.domain.com	critical	MS FrontPage Server Extension Vulnerability: remote debug	Web	<a href="#">CVE-2003-0822</a>	7.5	no
host1.domain.com	critical	Folder traversal in IIS (Double Decoding)	Web	<a href="#">CVE-2001-0333</a>	7.5	no
host1.domain.com	critical	Folder traversal in IIS (Unicode Translation)	Web	<a href="#">CVE-2000-0884</a>	7.5	no

				<a href="#">CVE-2000-0770</a>		
				<a href="#">CVE-2001-0151</a>		
				<a href="#">CVE-2001-0241</a>		
				<a href="#">CVE-2001-0500</a>		
				<a href="#">CVE-2001-0507</a>		
				<a href="#">CVE-2002-0869</a>		
host1.domain.com	critical	vulnerabilities in IIS 5	Web	<a href="#">CVE-2002-1180</a>	10.0	yes
				<a href="#">CVE-2002-1181</a>		
				<a href="#">CVE-2002-1182</a>		
				<a href="#">CVE-2003-0223</a>		
				<a href="#">CVE-2003-0224</a>		
				<a href="#">CVE-2003-0225</a>		
				<a href="#">CVE-2003-0226</a>		
host1.domain.com	critical	MailEnable HTTPMail vulnerability	Mail	<a href="#">CVE-2005-1348</a>	10.0	yes
				<a href="#">CVE-2005-2222</a>		
				<a href="#">CVE-2006-1338</a>		
host1.domain.com	critical	MS Site Server default account	Other	<a href="#">CVE-2002-1769</a>	7.5	no
				<a href="#">CVE-2002-2073</a>		
				<a href="#">CVE-2002-2081</a>		
host1.domain.com	critical	vulnerability in Windows Media Services (nsiislog.dll)	Web	<a href="#">CVE-2003-0227</a>	7.5	no
				<a href="#">CVE-2003-0349</a>		
host1.domain.com	critical	Windows Plug and Play vulnerability	Windows OS	<a href="#">CVE-2005-1983</a>	10.0	no
host1.domain.com	critical	RPC runtime library vulnerability	Windows OS	<a href="#">CVE-2003-0807</a>	5.1	no
				<a href="#">CVE-2003-0813</a>		
				<a href="#">CVE-2004-0116</a>		
				<a href="#">CVE-2004-0124</a>		
host1.domain.com	critical	Windows 2000 ASN1 buffer overflow	Windows OS	<a href="#">CVE-2003-0818</a>	7.5	no
host1.domain.com	critical	Windows 2000 RPC buffer overflow	Windows OS	<a href="#">CVE-2003-0352</a>	7.5	no
host1.domain.com	critical	Windows COM+ command execution vulnerability	Windows OS	<a href="#">CVE-2005-1978</a>	7.5	no
				<a href="#">CVE-2005-1979</a>		
				<a href="#">CVE-2005-1980</a>		
				<a href="#">CVE-2005-2119</a>		
host1.domain.com	critical	Windows SMB Transaction response buffer overflow	Windows OS	<a href="#">CVE-2005-0045</a>	7.5	no
host1.domain.com	critical	Windows SMB input validation vulnerability	Windows OS	<a href="#">CVE-2005-1206</a>	7.5	no
host1.domain.com	critical	Windows TCP/IP vulnerabilities	Windows OS	<a href="#">CVE-2004-0230</a>	7.5	yes
				<a href="#">CVE-2004-0790</a>		
				<a href="#">CVE-2004-1060</a>		
				<a href="#">CVE-2005-0048</a>		
				<a href="#">CVE-2005-0688</a>		
host1.domain.com	critical	Windows WMF gdi32.dll vulnerability	Windows OS	<a href="#">CVE-2005-4560</a>	7.5	no
host1.domain.com	critical	pointer corruption vulnerability in WINS replication service	Windows OS	<a href="#">CVE-2004-0567</a>	10.0	no
				<a href="#">CVE-2004-1080</a>		
host1.domain.com	critical	Worm detected (Code Red II)	Other			no
host1.domain.com	concern	Web server allows cross-site tracing	Web			yes
host1.domain.com	concern	Windows DNS server allows cache poisoning	DNS	<a href="#">CVE-2001-1452</a>	5.0	no
host1.domain.com	concern	Internet Explorer COM object memory corruption	Windows OS	<a href="#">CVE-2005-2127</a>	7.5	no
host1.domain.com	concern	Internet Explorer Create Text Range code injection	Windows OS	<a href="#">CVE-2006-1185</a>	10.0	no
				<a href="#">CVE-2006-1186</a>		
				<a href="#">CVE-2006-1188</a>		
				<a href="#">CVE-2006-1189</a>		
				<a href="#">CVE-2006-1190</a>		
				<a href="#">CVE-2006-1191</a>		
				<a href="#">CVE-2006-1192</a>		
				<a href="#">CVE-2006-1245</a>		
				<a href="#">CVE-2006-1359</a>		
				<a href="#">CVE-2006-1388</a>		
host1.domain.com	concern	Internet Explorer JPEG buffer overflow	Windows OS	<a href="#">CVE-2005-1988</a>	7.5	no
				<a href="#">CVE-2005-1989</a>		
				<a href="#">CVE-2005-1990</a>		
host1.domain.com	concern	Internet Explorer JS stack overflow	Windows OS	<a href="#">CVE-2006-0753</a>	7.5	no
				<a href="#">CVE-2006-0830</a>		
host1.domain.com	concern	Internet Explorer JavaScript vulnerability	Windows OS	<a href="#">CVE-2005-1790</a>	7.5	no
				<a href="#">CVE-2005-2829</a>		
				<a href="#">CVE-2005-2830</a>		
				<a href="#">CVE-2005-2831</a>		
host1.domain.com	concern	Internet Explorer PNG buffer overflow	Windows OS	<a href="#">CVE-2002-0648</a>	5.1	no
				<a href="#">CVE-2005-1211</a>		
host1.domain.com	concern	Internet Explorer URL parsing buffer overflow	Windows OS	<a href="#">CVE-2005-0553</a>	7.5	no
				<a href="#">CVE-2005-0554</a>		
				<a href="#">CVE-2005-0555</a>		

host1.domain.com	concern	Internet Explorer WMF handling vulnerability	Windows OS	<a href="#">CVE-2006-0020</a>	9.3	no
host1.domain.com	concern	vulnerability in License Logging Service	Windows OS	<a href="#">CVE-2005-0050</a>	7.5	no
host1.domain.com	concern	AxWebRemoveCtrl ActiveX control enabled	Web	<a href="#">CVE-2005-3693</a>	9.3	no
host1.domain.com	concern	CodeSupport ActiveX control enabled	Web	<a href="#">CVE-2005-3650</a>	9.3	no
host1.domain.com	concern	null session access using alternate pipes	Windows OS	<a href="#">CVE-2005-2150</a>	5.0	no
host1.domain.com	concern	Windows Plug and Play privilege elevation	Windows OS	<a href="#">CVE-2005-2120</a>	6.5	no
host1.domain.com	concern	Run key allows write access	Windows OS	<a href="#">CVE-1999-0589</a>	10.0	no
host1.domain.com	concern	Uninstall key allows write access	Windows OS	<a href="#">CVE-1999-0589</a>	10.0	no
host1.domain.com	concern	Windows telephony service vulnerability	Windows OS	<a href="#">CVE-2005-0058</a>	7.5	no
host1.domain.com	concern	DirectShow buffer overflow	Windows OS	<a href="#">CVE-2005-2128</a>	5.0	no
host1.domain.com	concern	HTML Application Host vulnerability in Windows shell	Windows OS	<a href="#">CVE-2005-0063</a>	7.5	no
host1.domain.com	concern	Microsoft Color Management Module buffer overflow	Windows OS	<a href="#">CVE-2005-1219</a>	7.5	no
host1.domain.com	concern	Microsoft Data Access Component vulnerability	Windows OS	<a href="#">CVE-2006-0003</a>	5.1	no
host1.domain.com	concern	Windows DHTML Editing Component vulnerability	Windows OS	<a href="#">CVE-2004-1319</a>	5.0	no
host1.domain.com	concern	Windows Explorer COM object command execution	Windows OS	<a href="#">CVE-2004-2289</a> <a href="#">CVE-2006-0012</a>	10.0	no
host1.domain.com	concern	Windows Hyperlink Object Library buffer overflow	Windows OS	<a href="#">CVE-2005-0057</a>	7.5	no
host1.domain.com	concern	Windows Kernel privilege elevation vulnerability	Windows OS	<a href="#">CVE-2005-2827</a>	7.2	no
host1.domain.com	concern	Windows Media Player plug-in EMBED vulnerability	Windows OS	<a href="#">CVE-2006-0005</a>	9.3	no
host1.domain.com	concern	Windows Web Fonts vulnerability	Windows OS	<a href="#">CVE-2006-0010</a>	7.5	no
host1.domain.com	concern	Windows shortcut file command execution	Windows OS	<a href="#">CVE-2005-2117</a> <a href="#">CVE-2005-2118</a> <a href="#">CVE-2005-2122</a>	10.0	no
host1.domain.com	concern	vulnerable WinZip version: 8.0	Other	<a href="#">CVE-2001-0449</a> <a href="#">CVE-2004-1465</a>	4.6	no
host1.domain.com	potential	guessable read community string	Networking/SNMP	<a href="#">CVE-1999-0516</a> <a href="#">CVE-1999-0517</a>	7.5	no
host1.domain.com	potential	Internet Explorer Shell.Explorer object enabled	Windows OS	<a href="#">CVE-2004-0985</a>	10.0	no
host1.domain.com	potential	Javaprx.dll access through Internet Explorer	Windows OS	<a href="#">CVE-2005-2087</a>	5.0	no
host1.domain.com	potential	last user name shown in login box	Windows OS	<a href="#">CVE-1999-0592</a>	10.0	no
host1.domain.com	potential	MailEnable Enterprise 1.04 may be vulnerable	Mail	<a href="#">CVE-2005-1013</a> <a href="#">CVE-2005-1781</a> <a href="#">CVE-2005-2223</a>	5.0	no
host1.domain.com	potential	possible vulnerability in MailEnable Enterprise IMAP 1.04	Mail	<a href="#">CVE-2005-1014</a> <a href="#">CVE-2005-1015</a> <a href="#">CVE-2005-2278</a> <a href="#">CVE-2005-3155</a> <a href="#">CVE-2005-3690</a> <a href="#">CVE-2005-3691</a> <a href="#">CVE-2005-3813</a> <a href="#">CVE-2005-3993</a> <a href="#">CVE-2005-4402</a> <a href="#">CVE-2005-4456</a> <a href="#">CVE-2005-4457</a> <a href="#">CVE-2006-0504</a>	10.0	no
host1.domain.com	potential	possible vulnerability in MailEnable Enterprise POP3 1.04	Mail	<a href="#">CVE-2006-1337</a>	7.5	no
host1.domain.com	potential	possible vulnerability in MailEnable POP3 0	Mail			yes
host1.domain.com	potential	excessive null session access	Windows OS	<a href="#">CVE-2000-1200</a>	5.0	no
host1.domain.com	potential	Possible ODBC RDS Vulnerability	Web	<a href="#">CVE-1999-1011</a> <a href="#">CVE-2002-1142</a>	10.0	no
host1.domain.com	potential	chargen could be used in UDP bomb	Networking/SNMP	<a href="#">CVE-1999-0103</a>	5.0	no
host1.domain.com	potential	pop receives password in clear	Mail			yes

host1.domain.com	potential	possible vulnerability in PPTP service	Other	<a href="#">CVE-2002-1214</a>	7.5	no
host1.domain.com	potential	SNMP is enabled and may be vulnerable	Networking/SNMP	<a href="#">CVE-1999-0615</a> <a href="#">CVE-2002-0012</a> <a href="#">CVE-2002-0013</a> <a href="#">CVE-2002-0053</a> <a href="#">CVE-2002-0796</a> <a href="#">CVE-2002-0797</a>	10.0	no
host1.domain.com	potential	TCP reset using approximate sequence number	Other	<a href="#">CVE-2004-0230</a>	5.0	no
host1.domain.com	potential	password complexity policy disabled	Windows OS	<a href="#">CVE-1999-0535</a>	10.0	no
host1.domain.com	potential	weak account lockout policy (0)	Windows OS	<a href="#">CVE-1999-0582</a>	5.0	no
host1.domain.com	potential	weak minimum password age policy (0 days)	Windows OS	<a href="#">CVE-1999-0535</a>	10.0	no
host1.domain.com	potential	weak minimum password length policy (0)	Windows OS	<a href="#">CVE-1999-0535</a>	10.0	no
host1.domain.com	potential	weak password history policy (0)	Windows OS	<a href="#">CVE-1999-0535</a>	10.0	no
host1.domain.com	potential	non-administrative users can act as part of the operating system	Windows OS	<a href="#">CVE-1999-0534</a>	4.6	no
host1.domain.com	potential	non-administrative users can bypass traverse checking	Windows OS	<a href="#">CVE-1999-0534</a>	4.6	no
host1.domain.com	potential	non-administrative users can create token object	Windows OS	<a href="#">CVE-1999-0534</a>	4.6	no
host1.domain.com	potential	auditing is disabled	Windows OS	<a href="#">CVE-1999-0575</a>	7.5	no
host1.domain.com	potential	Password never expires for user LDAP_Anonymous	Windows OS			yes
host1.domain.com	potential	Password never expires for user foobar	Windows OS			no
host1.domain.com	potential	Client Service for Netware vulnerability	Windows OS	<a href="#">CVE-2005-1985</a>	7.5	no
host1.domain.com	potential	Collaboration Data Objects vulnerability	Windows OS	<a href="#">CVE-2005-1987</a>	7.5	no
host1.domain.com	potential	FTP Client vulnerability	Windows OS	<a href="#">CVE-2005-2126</a>	2.6	yes
host1.domain.com	potential	Jet Database Engine input validation problems	Windows OS	<a href="#">CVE-2005-0944</a>	7.5	no
host1.domain.com	potential	Microsoft Agent spoofing vulnerability	Windows OS	<a href="#">CVE-2005-1214</a>	5.1	no
host1.domain.com	potential	Network Connection Manager vulnerability	Windows OS	<a href="#">CVE-2005-2307</a>	5.0	no
host1.domain.com	potential	Win2000 SP2 Security Rollup 1 not installed	Windows OS	<a href="#">CVE-1999-0662</a>	10.0	no
host1.domain.com	potential	Windows 2000 SP4 Update Rollup 1 not applied	Windows OS	<a href="#">CVE-2005-3168</a> <a href="#">CVE-2005-3169</a> <a href="#">CVE-2005-3170</a> <a href="#">CVE-2005-3171</a> <a href="#">CVE-2005-3172</a> <a href="#">CVE-2005-3173</a> <a href="#">CVE-2005-3174</a> <a href="#">CVE-2005-3175</a> <a href="#">CVE-2005-3176</a> <a href="#">CVE-2005-3177</a>	7.5	no
host1.domain.com	potential	Windows Media Player URL script execution	Windows OS	<a href="#">CVE-2003-1107</a>	5.1	no
host1.domain.com	potential	potential vulnerability in WINS	Windows OS	<a href="#">CVE-2003-0825</a>	7.5	no
host1.domain.com	service	17/TCP				
host1.domain.com	service	17/UDP				
host1.domain.com	service	42/TCP				
host1.domain.com	service	1027/TCP				
host1.domain.com	service	1028/TCP				
host1.domain.com	service	1031/UDP				
host1.domain.com	service	1033/TCP				
host1.domain.com	service	1035/UDP				
host1.domain.com	service	1036/TCP				
host1.domain.com	service	1037/UDP				
host1.domain.com	service	1038/TCP				
host1.domain.com	service	1039/TCP				
host1.domain.com	service	1041/UDP				
host1.domain.com	service	1043/UDP				
host1.domain.com	service	1645/UDP				