

ASV Scan Report - Executive Summary

Report Generated: July 27, 2010

1.0 Scan Information

Scan Customer Company:
Scan Date: July 22, 2010

ASV Company:
Scan Expires: October 20, 2010

2.0 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems	PCI Compliant?
10.7.0.2	SAINTLAB02	10.7.0.2	Microsoft Windows 2000 Workstation - Server Service Pack 4	12	7	21	FAIL

2.1 Vulnerabilities Noted for each IP Address

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

Host Name	Vulnerability / Service	CVE	PCI Severity	CVSSv2 Base Score	PCI Compliant?	PCI Reason
10.7.0.2	SQL Server account sa has no password	CVE-2000-1209	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	Windows Server Service Buffer Overrun	CVE-2006-3439	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	Windows Server Service MS08-067 buffer overflow	CVE-2008-4250	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	pointer corruption vulnerability in WINS replication service	CVE-2004-0567 CVE-2004-1080	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	vulnerable Microsoft NNTP version: 5.0.2195.2966	CVE-2004-0574	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	vulnerable version of SMB Server (MS10-012)	CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231	high	10.0	PASS	DOS vulnerabilities are PCI compliant

10.7.0.2	Microsoft SQL Server vulnerable version: 8.00.194	CVE-1999-0652 CVE-1999-0999 CVE-2000-0199 CVE-2000-0202 CVE-2000-0402 CVE-2000-0485 CVE-2000-0603 CVE-2000-1081 CVE-2000-1082 CVE-2000-1083 CVE-2000-1084 CVE-2000-1085 CVE-2000-1086 CVE-2000-1087 CVE-2000-1088 CVE-2001-0344 CVE-2001-0542 CVE-2001-0879 CVE-2002-0056 CVE-2002-0154 CVE-2002-0186 CVE-2002-0187 CVE-2002-0624 CVE-2002-0641 CVE-2002-0642 CVE-2002-0644 CVE-2002-0645 CVE-2002-0695 CVE-2002-0721 CVE-2002-0859 CVE-2002-0982 CVE-2002-1123 CVE-2002-1137 CVE-2002-1138 CVE-2002-1145 CVE-2003-0230 CVE-2003-0231 CVE-2003-0232	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	Possible vulnerabilities in IIS 5	CVE-2000-0770 CVE-2001-0151 CVE-2001-0241 CVE-2001-0500 CVE-2001-0507 CVE-2002-0869 CVE-2002-1180 CVE-2002-1181 CVE-2002-1182 CVE-2003-0223 CVE-2003-0224 CVE-2003-0225 CVE-2003-0226 CVE-2006-0026	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	SMTP may be a mail relay	CVE-1999-0512	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	SNMP is enabled and may be vulnerable	CVE-1999-0615 CVE-2002-0012 CVE-2002-0013 CVE-2002-0053 CVE-2002-0796 CVE-2002-0797	high	10.0	FAIL	CVSS score is over 3.9

10.7.0.2	possible buffer overflow in IIS 5.0 WebDAV	CVE-2001-0241 CVE-2001-0500 CVE-2003-0109	high	10.0	FAIL	CVSS score is over 3.9
10.7.0.2	WINS Could Allow Remote Code Execution	CVE-2009-1923 CVE-2009-1924	high	9.3	FAIL	CVSS score is over 3.9
10.7.0.2	Windows Media Unicast Service transport information buffer overflow	CVE-2010-0478	high	9.3	FAIL	CVSS score is over 3.9
10.7.0.2	Microsoft Internet Information Services FTP Server Remote Buffer Overflow	CVE-2009-2521 CVE-2009-3023	high	9.0	FAIL	CVSS score is over 3.9
10.7.0.2	Microsoft IIS WebDAV Request Directory Security Bypass	CVE-2009-1122 CVE-2009-1535	high	7.6	FAIL	CVSS score is over 3.9
10.7.0.2	Folder traversal in IIS (Double Decoding)	CVE-2001-0333	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	multiple vulnerabilities in IIS 5.0	CVE-2002-0071 CVE-2002-0072 CVE-2002-0073 CVE-2002-0074 CVE-2002-0075 CVE-2002-0079 CVE-2002-0147 CVE-2002-0148 CVE-2002-0149 CVE-2002-0150	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	Authentication flaw in Microsoft mail server	CVE-2001-0504 CVE-2002-0054	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	Is your LDAP secure?	CVE-2002-1378 CVE-2002-1379	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	Possible vulnerability in MS SQL Server Resolution Service	CVE-2002-0649 CVE-2002-0650 CVE-2002-0729	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	Possible vulnerability in Microsoft Terminal Server	CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	guessable read community string	CVE-1999-0516 CVE-1999-0517	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	possible Microsoft Exchange Buffer overflow in TNEF encoded messages	CVE-2006-0002	high	7.5	FAIL	CVSS score is over 3.9
10.7.0.2	vulnerable Microsoft mail server version: 5.0.2195.2966	CVE-2010-0024 CVE-2010-0025 CVE-2010-1689 CVE-2010-1690	medium	6.4	PASS	DOS vulnerabilities are PCI compliant
10.7.0.2	possible vulnerability in Apple Filing Protocol 2.0	CVE-2004-0430	medium	5.1	FAIL	CVSS score is over 3.9
10.7.0.2	denial of service in Windows SMTP service	CVE-2002-0055 CVE-2003-1106	medium	5.0	PASS	DOS vulnerabilities are PCI compliant
10.7.0.2	ASP.NET application folder information disclosure	CVE-2006-1300	medium	5.0	FAIL	CVSS score is over 3.9

10.7.0.2	Microsoft IIS Authentication Method Disclosed	CVE-2002-0419	medium	5.0	FAIL	CVSS score is over 3.9
10.7.0.2	NetBIOS Name Service information disclosure	CVE-2003-0661	medium	5.0	FAIL	CVSS score is over 3.9
10.7.0.2	Windows null session domain SID disclosure	CVE-2000-1200	medium	5.0	FAIL	CVSS score is over 3.9
10.7.0.2	chargen could be used in UDP bomb	CVE-1999-0103	medium	5.0	FAIL	CVSS score is over 3.9
10.7.0.2	possible WebDAV XML message handler denial of service	CVE-2003-0718	medium	5.0	FAIL	CVSS score is over 3.9
10.7.0.2	Possible vulnerability in LDAP over SSL	CVE-2001-0502	medium	4.6	FAIL	CVSS score is over 3.9
10.7.0.2	DNS cache snooping vulnerability		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
10.7.0.2	Web server allows cross-site tracing		low	2.6	FAIL	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD. SQL/XSS /SSL vulnerabilities are not PCI compliant
10.7.0.2	DNS server allows recursive queries		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
10.7.0.2	NetBIOS share enumeration using null session		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
10.7.0.2	Windows null session host SID disclosure		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.

10.7.0.2	DNS server allows zone transfers	CVE-1999-0532	low	0.0	FAIL	DNS zone transfers are not PCI compliant
10.7.0.2	ICMP timestamp requests enabled	CVE-1999-0524	low	0.0	PASS	

See the Resolution section of the PCI Detail report for instructions on correcting the above problems

2.2 Special Notes by IP Address

This table presents a list of special items detected on each host that require customer action.

Host Name	Note	Noted Item	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
10.7.0.2	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/removed. Please consult your ASV if you have questions about this Special Note.	remote access ports: 3389,500,2105,		