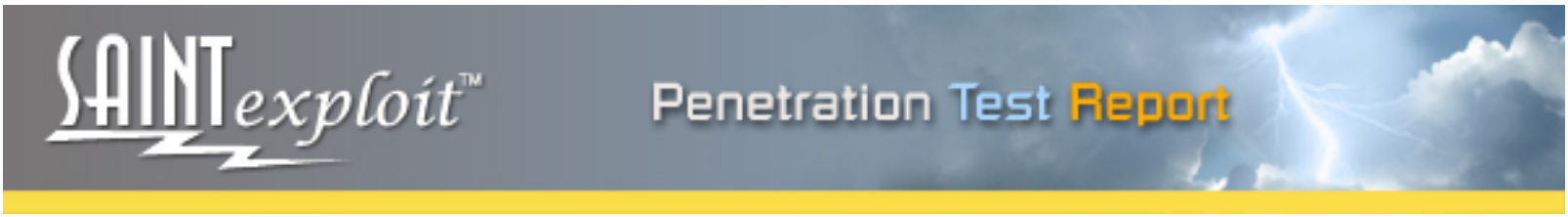

SAINTwriter Exploit Report

Report Generated: May 8, 2011

1.0 Introduction

On May 7, 2011, at 12:35 PM, a penetration test was conducted using the SAINTexploit™ 7.8 exploit tool. The scan discovered a total of three live hosts, and successfully performed one administrative level exploit, zero user level exploits, zero privilege elevation exploits, and zero client access exploits. The hosts and problems detected are discussed in greater detail in the following sections.

2.0 Overview

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

REMOTE ADMIN
Vulnerabilities successfully exploited by SAINTexploit to gain remote administrative privileges.

REMOTE USER
Vulnerabilities successfully exploited by SAINTexploit to gain remote unprivileged access.

PRIVILEGE ELEVATION
Vulnerabilities successfully exploited by SAINTexploit to gain elevated privileges after gaining remote unprivileged access.

CLIENT ACCESS
Vulnerabilities successfully exploited due to a user loading an exploit using a client application such as a browser or media player.

UNSUCCESSFUL
Vulnerabilities which were not successfully exploited.

The following tables present an overview of the hosts discovered on the network and the access level gained on each.

2.1 Host List

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

Host Name	Netbios Name	IP Address	Host Type	Remote Admin	Privilege Elevation	Remote User	Client Access	Unsuccessful Exploits
ls-chl-v2138.local		192.168.0.6	Linux 2.6.22	0	0	0	0	20
192.168.0.12	XP	192.168.0.12	Windows XP SP2	0	0	0	0	68

192.168.0.14	2K3	192.168.0.14	Windows Server 2003	1	0	0	0	16

2.2 Exploit List

This table presents an overview of the exploits executed on the network.

Host Name	Result	Vulnerability / Service	Class	CVE
ls-chl-v2138.local	unsuccessful exploit	AWStats configdir parameter command execution	Web	
ls-chl-v2138.local	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
ls-chl-v2138.local	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
ls-chl-v2138.local	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
ls-chl-v2138.local	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
ls-chl-v2138.local	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
ls-chl-v2138.local	unsuccessful exploit	Oracle Secure Backup login.php ora_osb_lcookie command execution	Web	
ls-chl-v2138.local	unsuccessful exploit	Oracle Secure Backup login.php rbtool command injection	Web	
ls-chl-v2138.local	unsuccessful exploit	Oracle Secure Backup property_box.php type parameter command execution	Web	
ls-chl-v2138.local	unsuccessful exploit	PHP Remote File Inclusion	Web	
ls-chl-v2138.local	unsuccessful exploit	phpBB viewtopic.php highlight parameter vulnerability	Web	
ls-chl-v2138.local	unsuccessful exploit	phpRPC decode function command execution	Web	
ls-chl-v2138.local	unsuccessful exploit	Samba call_trans2open buffer overflow	Other	
ls-chl-v2138.local	unsuccessful exploit	Snort DCE/RPC preprocessor buffer overflow	Other	CVE-2006-5276
ls-chl-v2138.local	unsuccessful exploit	SQL injection	Web	
ls-chl-v2138.local	unsuccessful exploit	SQL injection authentication bypass	Web	
ls-chl-v2138.local	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
ls-chl-v2138.local	unsuccessful exploit	Apache Tomcat JK Web Server Connector URI worker map buffer overflow	Web	
ls-chl-v2138.local	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
ls-chl-v2138.local	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
ls-chl-v2138.local	service	873/TCP		
ls-chl-v2138.local	service	3689/TCP		
ls-chl-v2138.local	service	8873/TCP		
ls-chl-v2138.local	service	9050/TCP		
ls-chl-v2138.local	service	SMB		
ls-chl-v2138.local	service	WWW		

ls-chl-v2138.local	service	WWW (Secure)		
ls-chl-v2138.local	service	WWW (non-standard port 3689)		
ls-chl-v2138.local	service	WWW (non-standard port 9050)		
ls-chl-v2138.local	service	bootpc (68/UDP)		
ls-chl-v2138.local	service	discard (9/UDP)		
ls-chl-v2138.local	service	http (80/TCP)		
ls-chl-v2138.local	service	https (443/TCP)		
ls-chl-v2138.local	service	microsoft-ds (445/TCP)		
ls-chl-v2138.local	service	netbios-ssn (139/TCP)		
ls-chl-v2138.local	service	printer (515/TCP)		
ls-chl-v2138.local	service	tftp (69/UDP)		
ls-chl-v2138.local	info	not vulnerable to cross-site scripting: /webbrowse-e61 /webbrowse-e61/upload		
ls-chl-v2138.local	info	not vulnerable to cross-site scripting: /webbrowse-n95 /webbrowse-n95/upload		
ls-chl-v2138.local	info	not vulnerable to cross-site scripting: /webbrowse /webbrowse/upload		
192.168.0.12	unsuccessful exploit	Adobe Flash Player Flash Content Parsing Code Execution	Other	CVE-2010-3654
192.168.0.12	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
192.168.0.12	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
192.168.0.12	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
192.168.0.12	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
192.168.0.12	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
192.168.0.12	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
192.168.0.12	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
192.168.0.12	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
192.168.0.12	unsuccessful exploit	Adobe Flash Player authplay.dll vulnerability	Other	CVE-2009-1862
192.168.0.12	unsuccessful exploit	Adobe Flash Player callMethod Bytecode Memory Corruption	Other	CVE-2011-0611
192.168.0.12	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
192.168.0.12	unsuccessful exploit	HP Data Protector Manager MMD Service Stack Buffer Overflow	Other	
192.168.0.12	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
192.168.0.12	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
192.168.0.12	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
192.168.0.12	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
192.168.0.12	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
192.168.0.12	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
192.168.0.12	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219

192.168.0.12	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
192.168.0.12	unsuccessful exploit	Internet Explorer iepeers.dll use-after-free vulnerability	Browsers	CVE-2010-0806
192.168.0.12	unsuccessful exploit	Internet Explorer IFRAME buffer overflow	Browsers	CVE-2004-1050
192.168.0.12	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
192.168.0.12	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
192.168.0.12	unsuccessful exploit	JRun mod_jrun WriteToLog buffer overflow	Web	CVE-2004-0646
192.168.0.12	unsuccessful exploit	Microsoft WMI Administrative Tools ActiveX Control AddContextRef vulnerability	Other	CVE-2010-3973
192.168.0.12	unsuccessful exploit	Microsoft Windows Movie Maker IsValidWMToolsStream buffer overflow	Other	CVE-2010-0265
192.168.0.12	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
192.168.0.12	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
192.168.0.12	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
192.168.0.12	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
192.168.0.12	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
192.168.0.12	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
192.168.0.12	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
192.168.0.12	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
192.168.0.12	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067

192.168.0.12	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
192.168.0.12	unsuccessful exploit	Windows password weakness	Passwords	CVE-1999-0503
192.168.0.12	unsuccessful exploit	Snort Back Orifice Pre-Processor buffer overflow	Other	CVE-2005-3252
192.168.0.12	unsuccessful exploit	Snort DCE/RPC preprocessor buffer overflow	Other	CVE-2006-5276
192.168.0.12	unsuccessful exploit	Apache Struts2 XWork ParameterInterceptor security bypass	Web	CVE-2010-1870
192.168.0.12	unsuccessful exploit	Symantec Alert Management System Intel Alert Handler command execution	Other	
192.168.0.12	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
192.168.0.12	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
192.168.0.12	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
192.168.0.12	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
192.168.0.12	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
192.168.0.12	unsuccessful exploit	Windows LSASS buffer overflow	Windows OS	CVE-2003-0533
192.168.0.12	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
192.168.0.12	unsuccessful exploit	Windows RPC DCOM interface buffer overflow	Windows OS	CVE-2003-0352
192.168.0.12	unsuccessful exploit	Windows RRAS memory corruption vulnerability	Windows OS	CVE-2006-2370
192.168.0.12	unsuccessful exploit	Windows Server Service buffer overflow	Windows OS	CVE-2006-3439
192.168.0.12	unsuccessful exploit	Windows Server Service buffer overflow MS08-067	Windows OS	CVE-2008-4250
192.168.0.12	unsuccessful exploit	Windows Thumbnail View CreateSizedDIBSECTION buffer overflow	Windows OS	CVE-2010-3970
192.168.0.12	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
192.168.0.12	unsuccessful exploit	Wireshark LWRES dissector buffer overflow	Other	CVE-2010-0304
192.168.0.12	service	1900/UDP		
192.168.0.12	service	SMB		
192.168.0.12	service	WWW (non-standard port 2869)		
192.168.0.12	service	epmap (135/TCP)		
192.168.0.12	service	isakmp (500/UDP)		
192.168.0.12	service	microsoft-ds (445/TCP)		
192.168.0.12	service	microsoft-ds (445/UDP)		
192.168.0.12	service	netbios-dgm (138/UDP)		
192.168.0.12	service	netbios-ns (137/UDP)		
192.168.0.12	service	ntp (123/UDP)		
192.168.0.14	remote admin	Windows RPC DCOM interface buffer overflow	Windows OS	CVE-2003-0352
192.168.0.14	unsuccessful exploit	Computer Associates Alert Notification Server buffer overflow	Other	CVE-2007-3825
192.168.0.14	unsuccessful exploit	Computer Associates Alert Notification Server opcode 23 buffer overflow	Other	CVE-2007-4620

192.168.0.14	unsuccessful exploit	HP Data Protector Manager MMD Service Stack Buffer Overflow	Other	
192.168.0.14	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
192.168.0.14	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
192.168.0.14	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
192.168.0.14	unsuccessful exploit	Novell Client nwspool.dll EnumPrinters buffer overflow	Other	CVE-2008-0639
192.168.0.14	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
192.168.0.14	unsuccessful exploit	Windows password weakness	Passwords	CVE-1999-0503
192.168.0.14	unsuccessful exploit	Snort Back Orifice Pre-Processor buffer overflow	Other	CVE-2005-3252
192.168.0.14	unsuccessful exploit	Apache Struts2 XWork ParameterInterceptor security bypass	Web	CVE-2010-1870
192.168.0.14	unsuccessful exploit	Symantec Alert Management System Intel Alert Handler command execution	Other	
192.168.0.14	unsuccessful exploit	Windows DNS server RPC management interface buffer overflow	RPC	CVE-2007-1748
192.168.0.14	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
192.168.0.14	unsuccessful exploit	Windows Server Service buffer overflow MS08-067	Windows OS	CVE-2008-4250
192.168.0.14	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
192.168.0.14	service	1025/TCP		
192.168.0.14	service	1026/TCP		
192.168.0.14	service	1028/UDP		
192.168.0.14	service	SMB		
192.168.0.14	service	epmap (135/TCP)		
192.168.0.14	service	isakmp (500/UDP)		
192.168.0.14	service	microsoft-ds (445/TCP)		
192.168.0.14	service	microsoft-ds (445/UDP)		
192.168.0.14	service	netbios-dgm (138/UDP)		
192.168.0.14	service	netbios-ns (137/UDP)		
192.168.0.14	service	ntp (123/UDP)		
192.168.0.14	info	Found password hash: Administrator : 500 : 4bd0f3d13d038cc3935d0e10d22e87c7 : bd09d74cbc4777b88b0ea5a7df135b03		
192.168.0.14	info	Found password hash: Guest : 501 : 31d6cfe0d16ae931b73c59d7e0c089c0 : aad3b435b51404eeaad3b435b51404ee		
192.168.0.14	info	Found password hash: SUPPORT_388945a0 : 1001 : 5502b52ab1b5d056655969b871c44809 : aad3b435b51404eeaad3b435b51404ee		

Scan Session: saint-data; Scan Policy: heavy; Scan Data Set: 7 May 2011 12:35