

Contents

- [Introduction](#)
- ▣ [Summary](#)
- ▣ [Overview](#)
- ▣ [Details](#)



Vulnerability Assessment Report

New Report

Save Report

July 8, 2009

1.0 Introduction

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.

2.0 Summary

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.

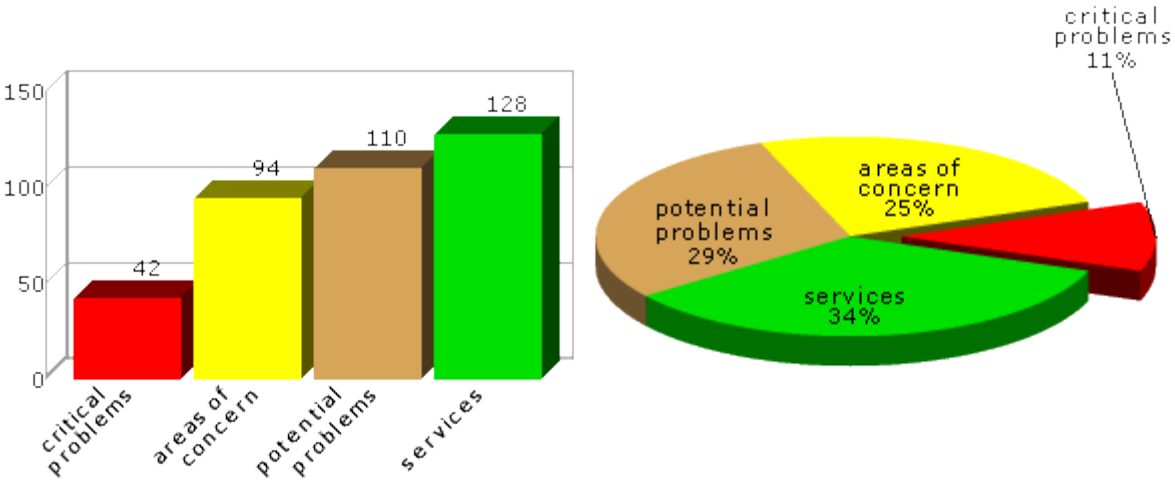
SERVICES

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 sections below summarize the results of the scan.

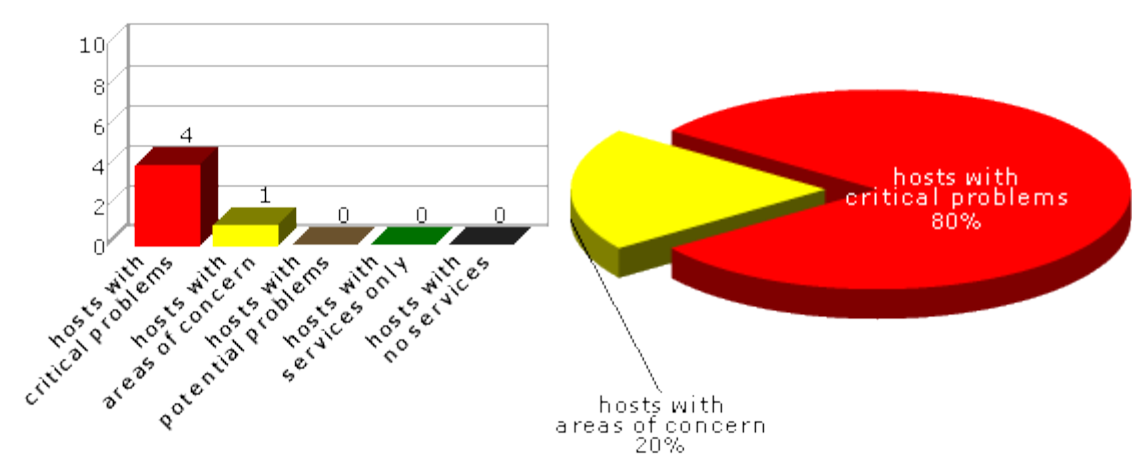
2.1 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level.



2.2 Hosts by Severity

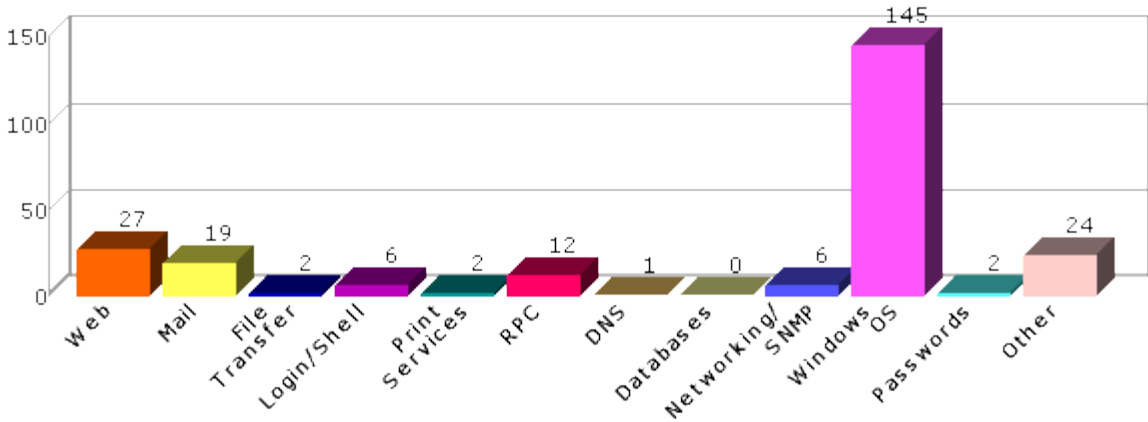
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

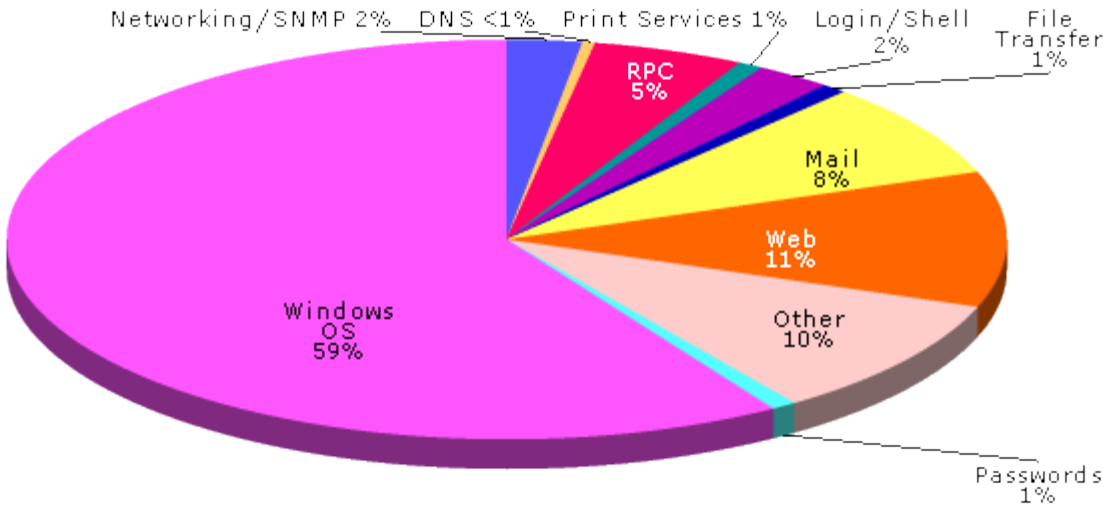


2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each of the following classes.

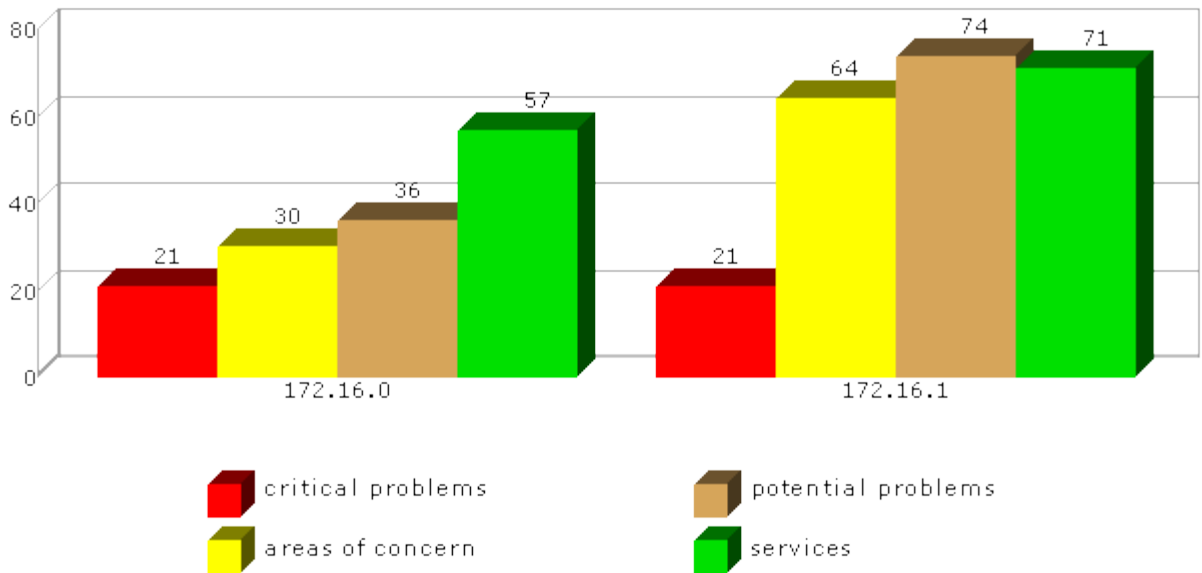
Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes





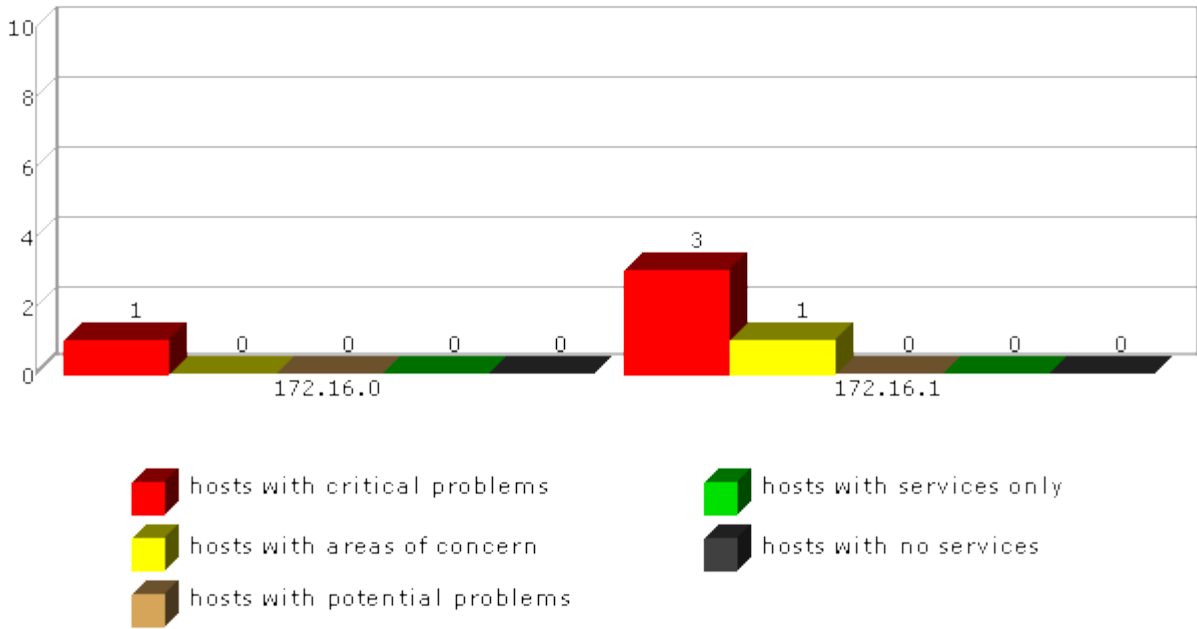
2.4 Vulnerabilities by Subnet

This section shows the number of vulnerabilities detected at each severity level for each subnet that was scanned.



2.5 Hosts by Subnet

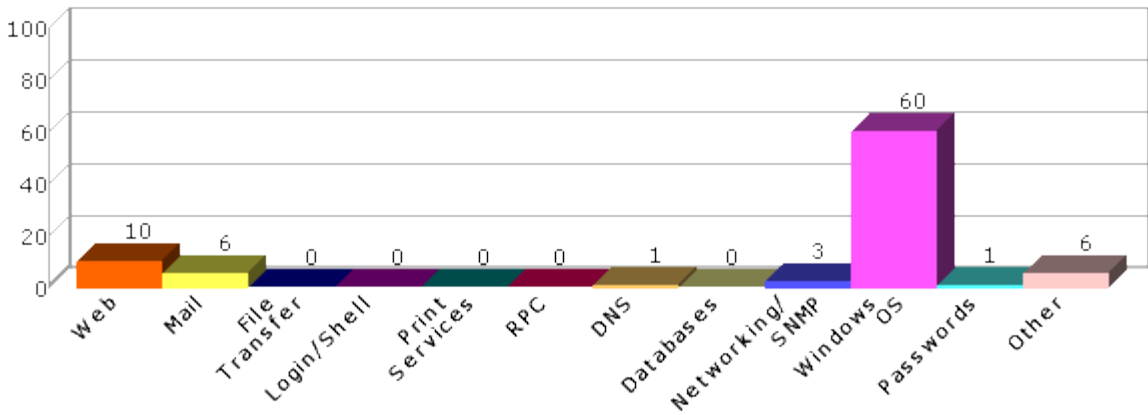
This section shows the overall number of hosts detected at each severity level for each subnet that was scanned. The severity level of a host is defined as the highest vulnerability severity level detected on that host.



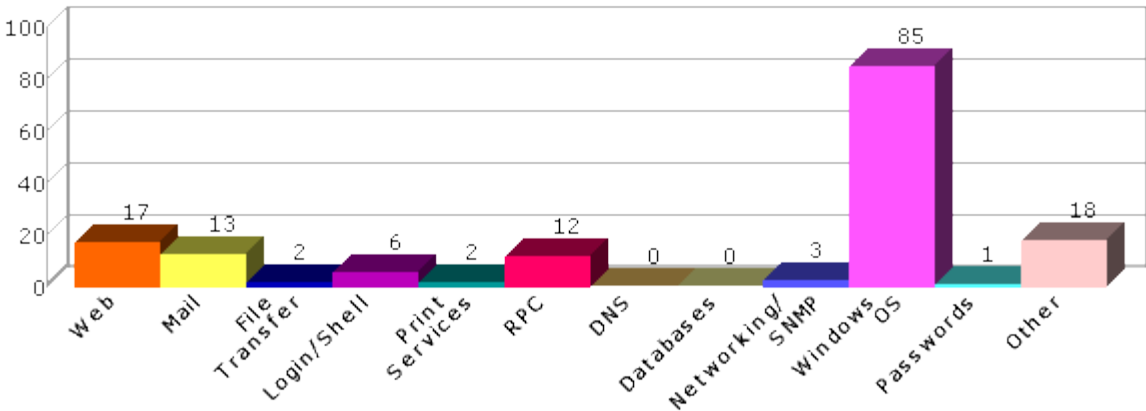
2.6 Vulnerabilities per Class by Subnet

This section shows the overall number of vulnerabilities detected in each vulnerability class for each subnet that was scanned.

172.16.0



172.16.1



3.0 Overview

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

3.1 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
host1.domain.com	HOST1	172.16.0.1	Windows 2000 Service Pack 1	21	30	36
host2.domain.com	HOST2	172.16.1.2	Windows Server 2003	8	29	31
host3.domain.com		172.16.1.3	Sun Solaris 2.5.1 - 9 (SunOS 5.9)	11	4	17
host4.domain.com	HOST4	172.16.1.4	Windows XP Service Pack 2	0	20	19
host5.domain.com		172.16.1.5	Linux 2.4.20-28.7 - Red Hat	2	11	7

3.2 Vulnerability List

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

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
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	CVE-2003-0824	no
host1.domain.com	critical	MS FrontPage Server Extension Vulnerability: remote debug	Web	CVE-2003-0822	yes
host1.domain.com	critical	Folder traversal in IIS (Double Decoding)	Web	CVE-2001-0333	yes
host1.domain.com	critical	Folder traversal in IIS (Unicode Translation)	Web	CVE-2000-0884	yes
host1.domain.com	critical	vulnerabilities in IIS 5	Web	CVE-2000-0770 CVE-2001-0151 CVE-2001-0241 CVE-2001-0500 CVE-2001-0507 CVE-2002-0869 CVE-2002-1180 CVE-2002-1181	yes



				CVE-2002-1182 CVE-2003-0223 CVE-2003-0224 CVE-2003-0225 CVE-2003-0226	
host1.domain.com	critical	MailEnable HTTPMail vulnerability	Mail	CVE-2005-1348 CVE-2005-2222 CVE-2006-1338	yes
host1.domain.com	critical	MS Site Server default account	Other	CVE-2002-1769 CVE-2002-2073 CVE-2002-2081	no
host1.domain.com	critical	vulnerability in Windows Media Services (nsiislog.dll)	Web	CVE-2003-0227 CVE-2003-0349	no
host1.domain.com	critical	Windows Plug and Play vulnerability	Windows OS	CVE-2005-1983	yes
host1.domain.com	critical	RPC runtime library vulnerability	Windows OS	CVE-2003-0807 CVE-2003-0813 CVE-2004-0116 CVE-2004-0124	no
host1.domain.com	critical	Windows 2000 ASN1 buffer overflow	Windows OS	CVE-2003-0818	no
host1.domain.com	critical	Windows 2000 RPC buffer overflow	Windows OS	CVE-2003-0352	yes
host1.domain.com	critical	Windows COM+ command execution vulnerability	Windows OS	CVE-2005-1978 CVE-2005-1979 CVE-2005-1980 CVE-2005-2119	no
host1.domain.com	critical	Windows SMB Transaction response buffer overflow	Windows OS	CVE-2005-0045	no
host1.domain.com	critical	Windows SMB input validation vulnerability	Windows OS	CVE-2005-1206	no
host1.domain.com	critical	Windows TCP/IP vulnerabilities	Windows OS	CVE-2004-0230 CVE-2004-0790 CVE-2004-1060 CVE-2005-0048 CVE-2005-0688	no
host1.domain.com	critical	Windows WMF gdi32.dll vulnerability	Windows OS	CVE-2005-4560	yes
host1.domain.com	critical	pointer corruption vulnerability in WINS replication service	Windows OS	CVE-2004-0567 CVE-2004-1080	yes
host1.domain.com	critical	Worm detected (Code Red II)	Other		no
host1.domain.com	concern	Web server allows cross-site tracing	Web		no
host1.domain.com	concern	Windows DNS server allows cache poisoning	DNS	CVE-2001-1452	no
host1.domain.com	concern	Internet Explorer COM object memory corruption	Windows OS	CVE-2005-2127	no
host1.domain.com	concern	Internet Explorer Create Text Range code injection	Windows OS	CVE-2006-1185 CVE-2006-1186 CVE-2006-1188 CVE-2006-1189 CVE-2006-1190 CVE-2006-1191 CVE-2006-1192 CVE-2006-1245 CVE-2006-1359 CVE-2006-1388	yes
host1.domain.com	concern	Internet Explorer JPEG buffer overflow	Windows OS	CVE-2005-1988 CVE-2005-1989 CVE-2005-1990	yes
host1.domain.com	concern	Internet Explorer JS stack overflow	Windows OS	CVE-2006-0753 CVE-2006-0830	no
host1.domain.com	concern	Internet Explorer JavaScript vulnerability	Windows OS	CVE-2005-1790 CVE-2005-2829 CVE-2005-2830 CVE-2005-2831	yes
host1.domain.com	concern	Internet Explorer PNG buffer overflow	Windows OS	CVE-2002-0648 CVE-2005-1211	no
host1.domain.com	concern	Internet Explorer URL parsing buffer overflow	Windows OS	CVE-2005-0553 CVE-2005-0554 CVE-2005-0555	yes
host1.domain.com	concern	Internet Explorer WMF handling vulnerability	Windows OS	CVE-2006-0020	no
host1.domain.com	concern	vulnerability in License Logging Service	Windows OS	CVE-2005-0050	no
host1.domain.com	concern	AxWebRemoveCtrl ActiveX control enabled	Web	CVE-2005-3693	no
host1.domain.com	concern	CodeSupport ActiveX control enabled	Web	CVE-2005-3650	no
		null session access			