

# Executive Vulnerability Assessment Report

Report Generated: April 6, 2011

## 1.0 Introduction

On March 19, 2011, at 9:48 PM, a PCI vulnerability assessment was conducted using the SAINT 7.7.5 vulnerability scanner. The scan discovered a total of 22 live hosts, and detected 48 critical problems, 29 areas of concern, and 274 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.

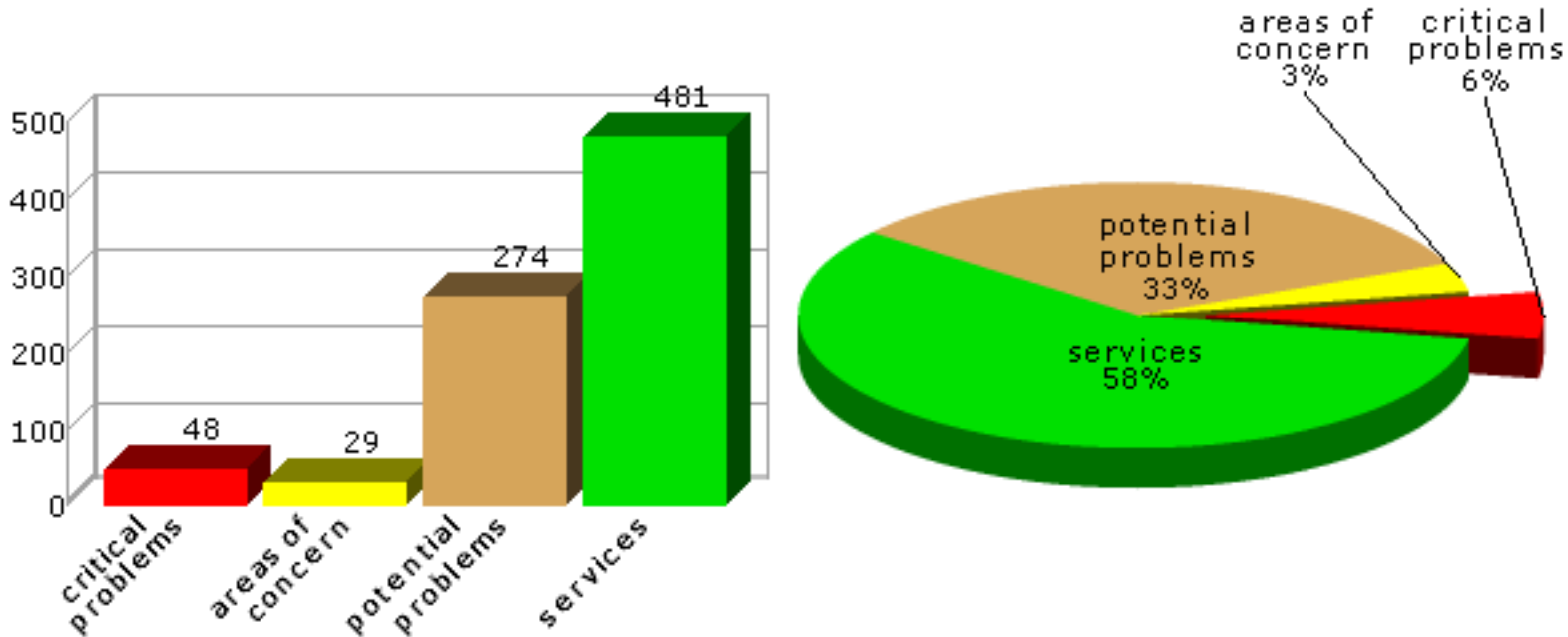
### **SERVICES**

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.

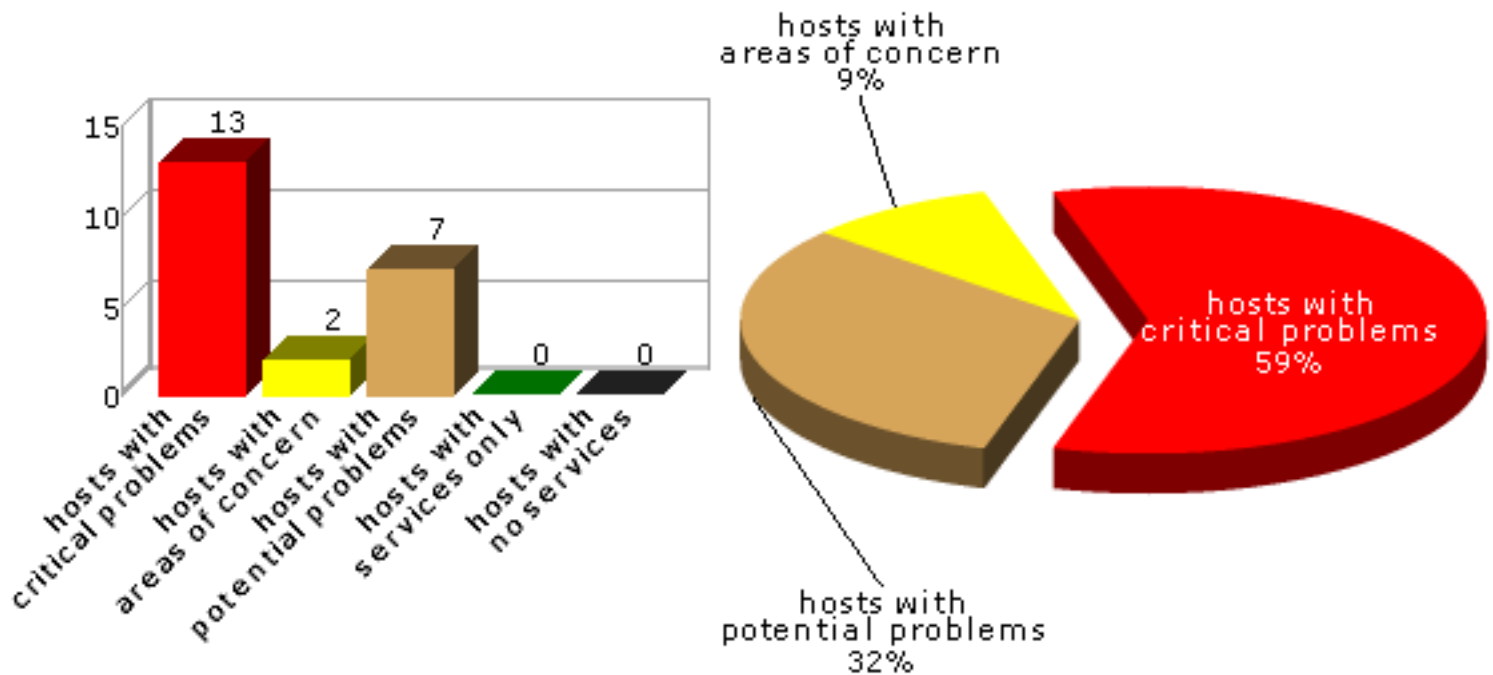
## 2.1 Vulnerabilities by Severity

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.

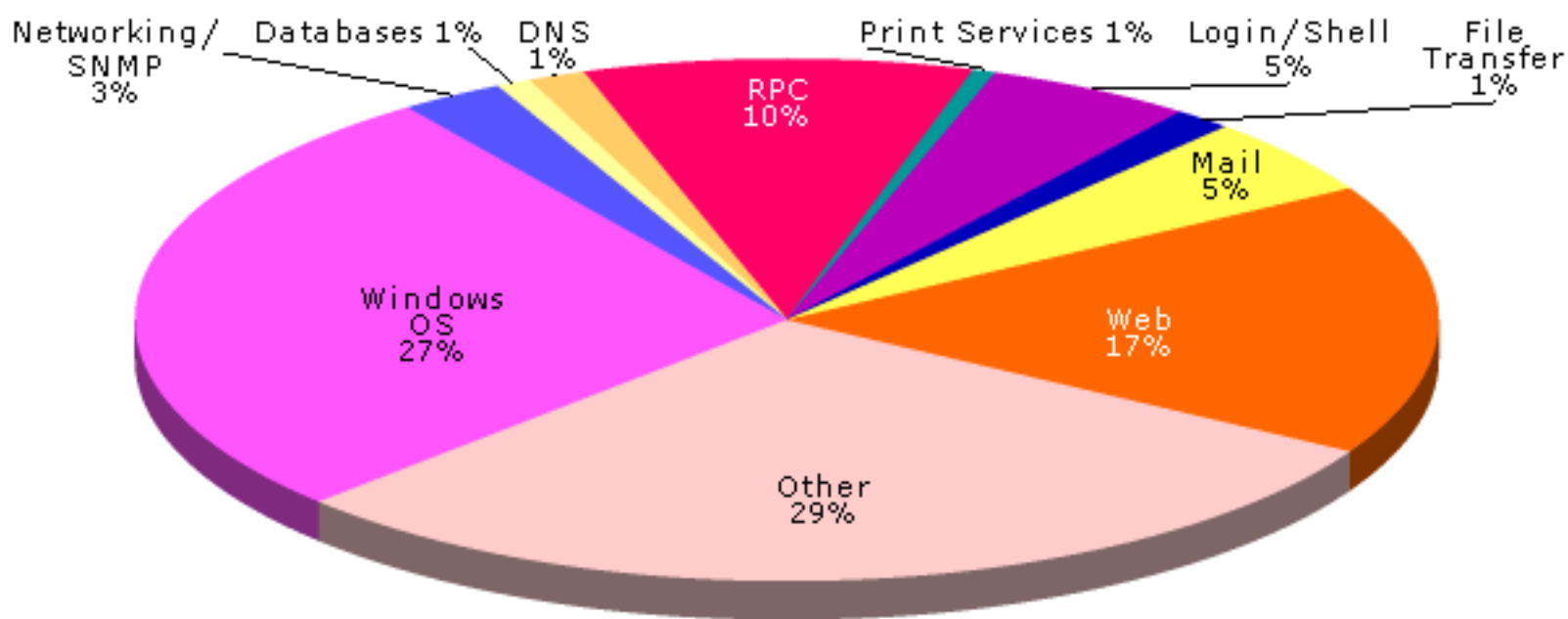
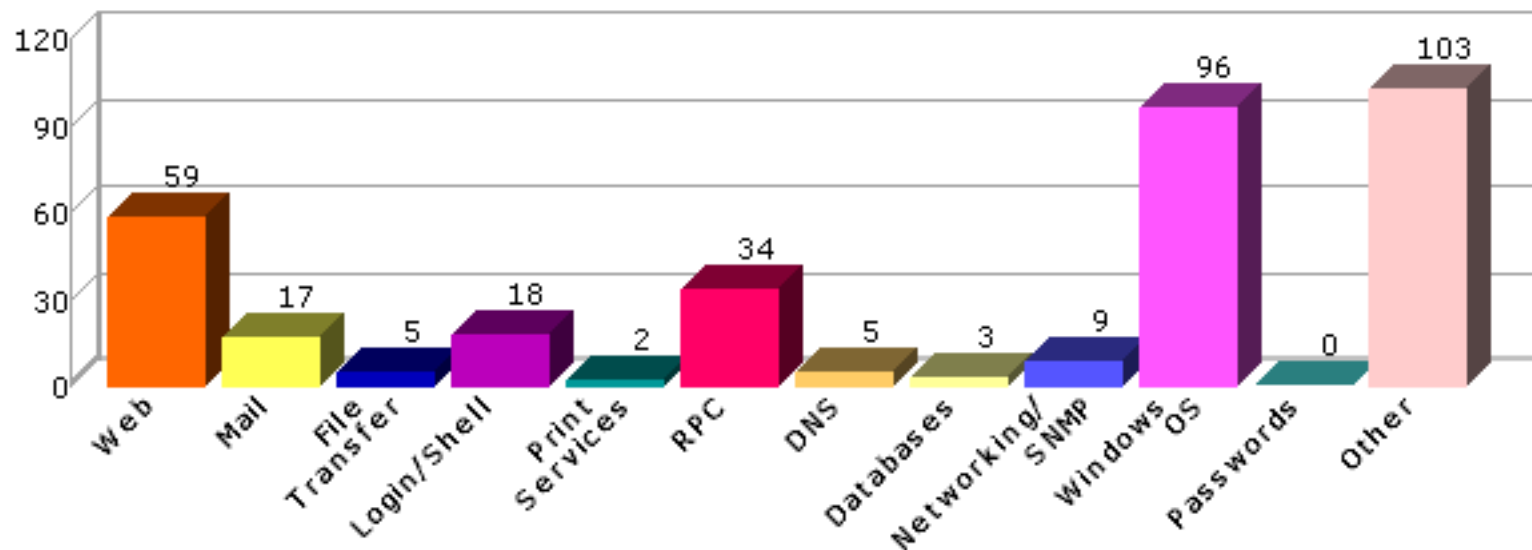


## 2.3 Vulnerabilities by Class

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

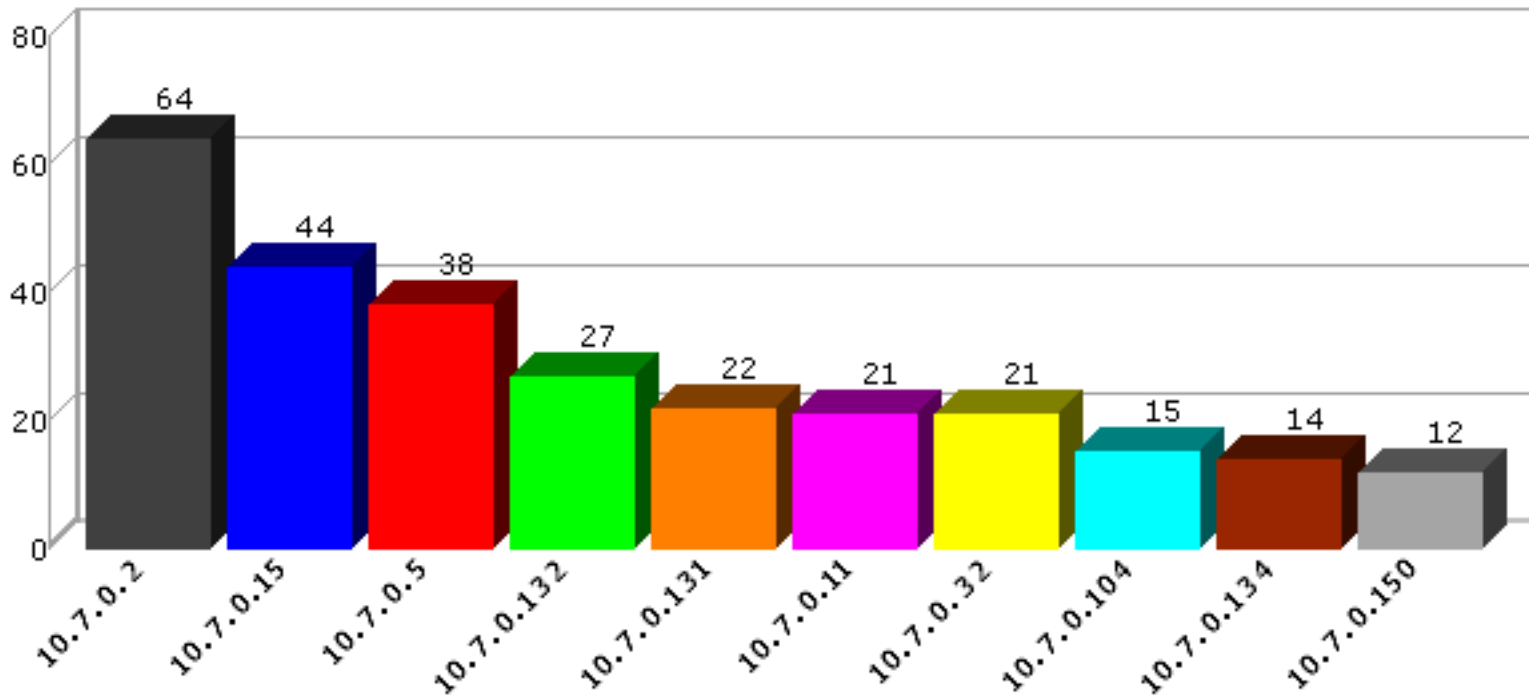
Class	Description
<b>Web</b>	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
<b>Mail</b>	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
<b>File Transfer</b>	Vulnerabilities in FTP and TFTP services
<b>Login/Shell</b>	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
<b>Print Services</b>	Vulnerabilities in lpd and other print daemons
<b>RPC</b>	Vulnerabilities in Remote Procedure Call services

<b>DNS</b>	Vulnerabilities in Domain Name Services
<b>Databases</b>	Vulnerabilities in database services
<b>Networking/SNMP</b>	Vulnerabilities in routers, switches, firewalls, or any SNMP service
<b>Windows OS</b>	Missing hotfixes or vulnerabilities in the registry or SMB shares
<b>Passwords</b>	Missing or easily guessed user passwords
<b>Other</b>	Any vulnerability which does not fit into one of the above classes



## 2.4 Top 10 Vulnerable Hosts

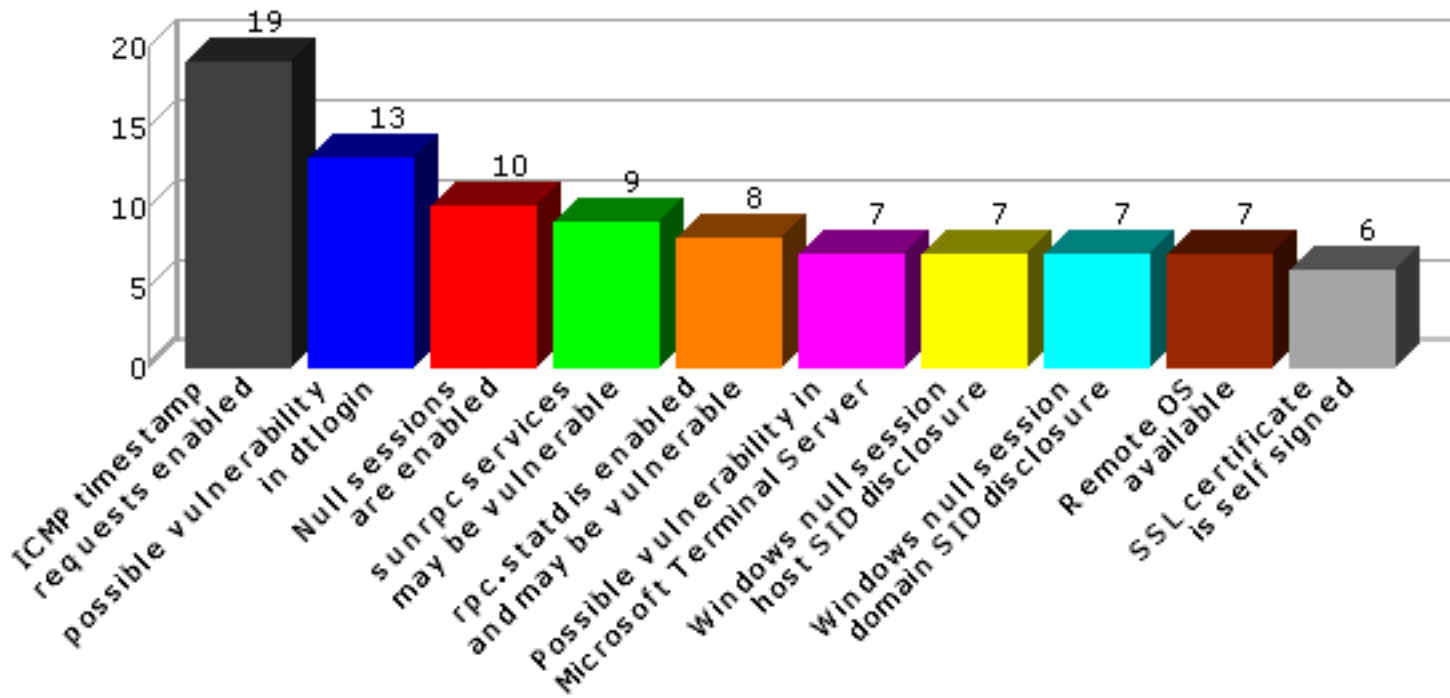
This section shows the most vulnerable hosts detected, and the number of vulnerabilities detected on them.



#	Host Name	Host Type	Vulnerabilities
1	10.7.0.2	Windows 2000 SP2	64
2	10.7.0.15	Windows 2000 SP2	44
3	10.7.0.5	SunOS 5.6	38
4	10.7.0.132	Windows	27
5	10.7.0.131	Windows	22
6	10.7.0.11	Windows Server 2003 SP1	21
7	10.7.0.32	Windows	21
8	10.7.0.104	Windows XP	15
9	10.7.0.134		14
10	10.7.0.150	Windows Server 2008 R2 Enterprise	12

## 2.5 Top 10 Vulnerabilities

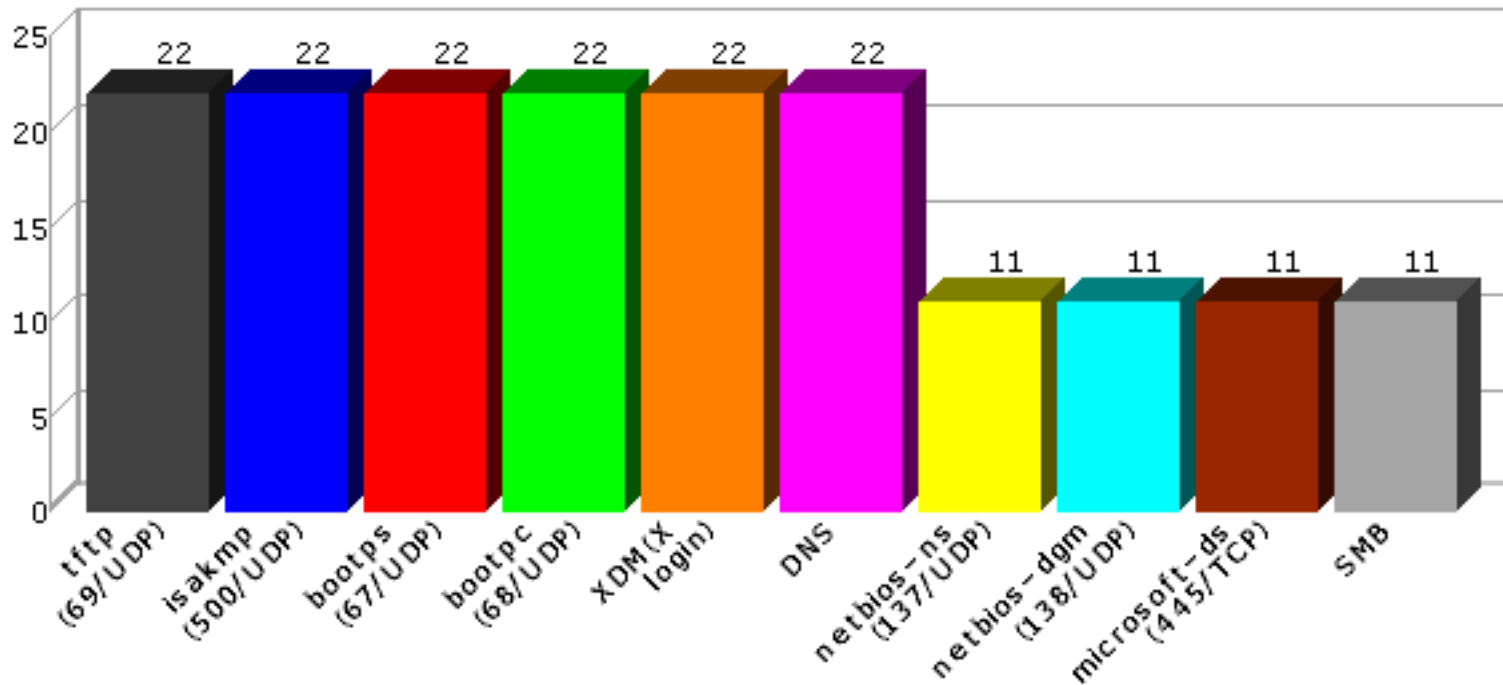
This section shows the most common vulnerabilities detected, and the number of hosts on which they were detected.



#	Vulnerability	Hosts
1	ICMP timestamp requests enabled	19
2	possible vulnerability in dtlogin	13
3	Null sessions are enabled	10
4	sunrpc services may be vulnerable	9
5	rpc.statd is enabled and may be vulnerable	8
6	Possible vulnerability in Microsoft Terminal Server	7
7	Windows null session host SID disclosure	7
8	Windows null session domain SID disclosure	7
9	Remote OS available	7
10	SSL certificate is self signed	6

## 2.6 Top 10 Services

This section shows the most common services detected, and the number of hosts on which they were detected.



#	Service	Hosts
1	tftp (69/UDP)	22
2	isakmp (500/UDP)	22
3	bootps (67/UDP)	22
4	bootpc (68/UDP)	22
5	XDM (X login)	22
6	DNS	22
7	netbios-ns (137/UDP)	11
8	netbios-dgm (138/UDP)	11
9	microsoft-ds (445/TCP)	11
10	SMB	11

### 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	Exploitable
10.7.0.2	SAINTLAB02	10.7.0.2	Windows 2000 SP2	14	6	44	15
10.7.0.4		10.7.0.4	FreeBSD	1	0	5	0
10.7.0.5		10.7.0.5	SunOS 5.6	12	5	21	3
10.7.0.9		10.7.0.9	Windows	0	0	6	0
10.7.0.10		10.7.0.10	Linux	1	0	5	0

10.7.0.11	WIN2003UNPATCH	10.7.0.11	Windows Server 2003 SP1	5	4	12	1
10.7.0.14	XPPROUNPATCHED	10.7.0.14	Windows XP	1	0	3	1
10.7.0.15	TRAINING2	10.7.0.15	Windows 2000 SP2	4	5	35	6
10.7.0.31		10.7.0.31		0	1	7	0
10.7.0.32	UBUNTU910UNPATC	10.7.0.32	Windows	1	1	19	0
10.7.0.101		10.7.0.101	Windows	0	0	2	0
10.7.0.104	XPSP3PATCHED	10.7.0.104	Windows XP	1	2	12	1
10.7.0.131	UBUNTU9	10.7.0.131	Windows	2	1	19	0
10.7.0.132	UBUNTU910PATCHE	10.7.0.132	Windows	3	2	22	0
10.7.0.134		10.7.0.134		0	2	12	0
10.7.0.138		10.7.0.138		1	0	6	0
10.7.0.142		10.7.0.142		0	0	5	0
10.7.0.145		10.7.0.145		0	0	6	0
10.7.0.150	WIN-IQF3U12CJA5	10.7.0.150	Windows Server 2008 R2 Enterprise	0	0	12	0
10.7.0.151	WIN-IQF3U12CJA5	10.7.0.151	Windows Server 2008 R2 Enterprise	0	0	12	0
10.7.0.153		10.7.0.153		2	0	6	0
10.7.0.250		10.7.0.250		0	0	3	0

Scan Session: SAINT Honeypot VA; Scan Policy: PCI; Scan Data Set: 19 March 2011 21:48

Copyright 2001-2011 SAINT Corporation. All rights reserved.