



Windows Desktop Antivirus Status Report

Report Generated: December 14, 2015

1 Introduction

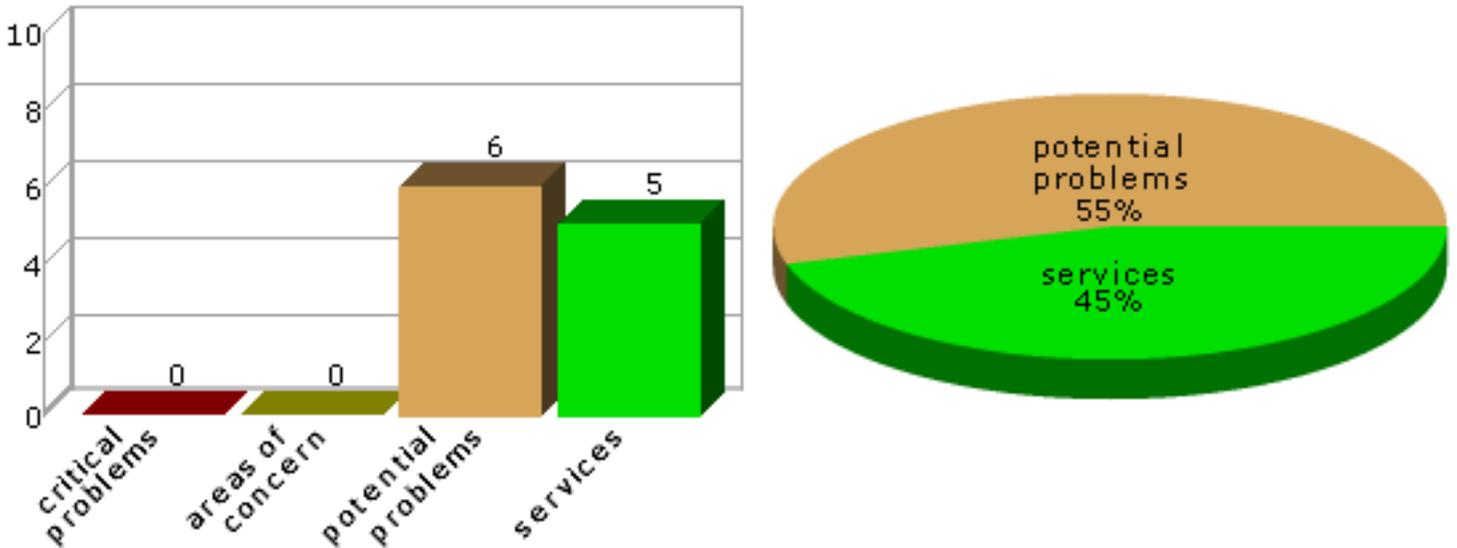
On December 14, 2015, at 5:21 PM, an Anti-virus Information assessment was conducted using the SAINT 8.9.28 vulnerability scanner. The scan discovered a total of six live hosts, and detected zero critical problems, zero areas of concern, and six potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

The sections below summarize the results of the scan.

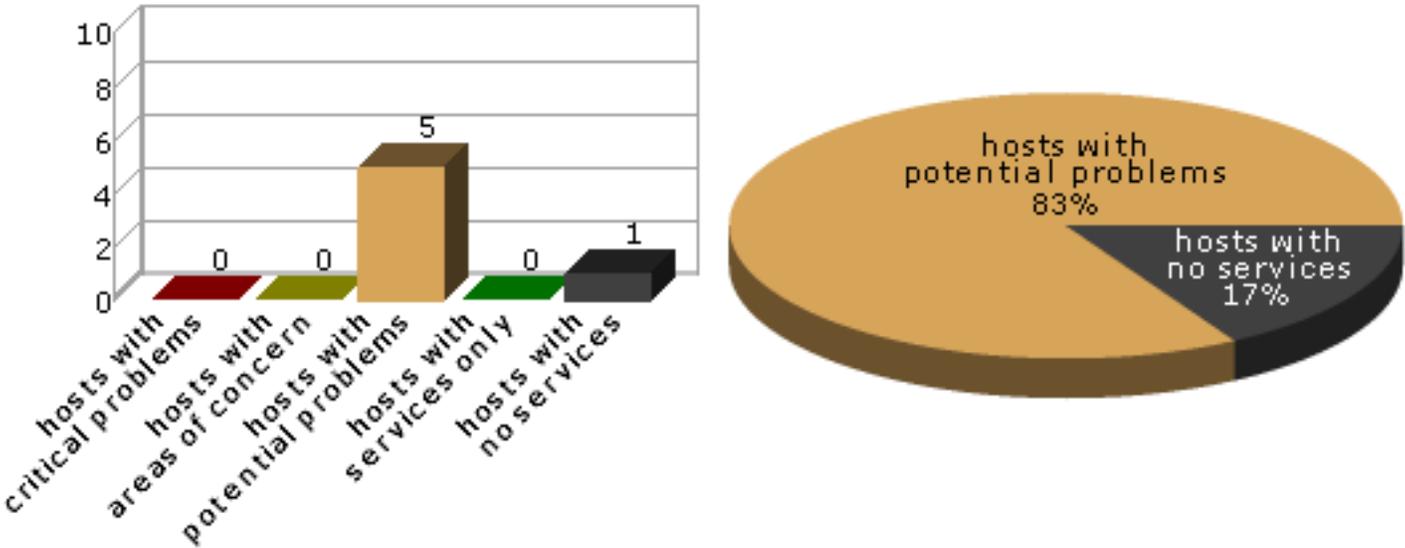
2.1 Vulnerabilities by Severity

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



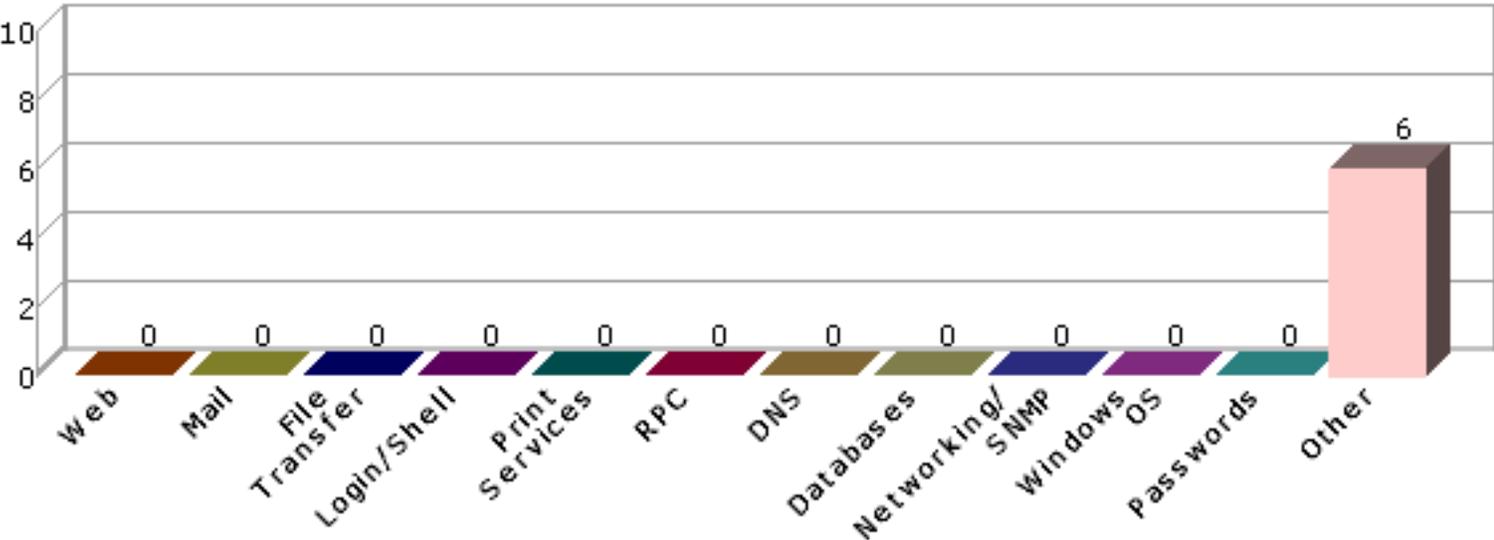
2.2 Hosts by Severity

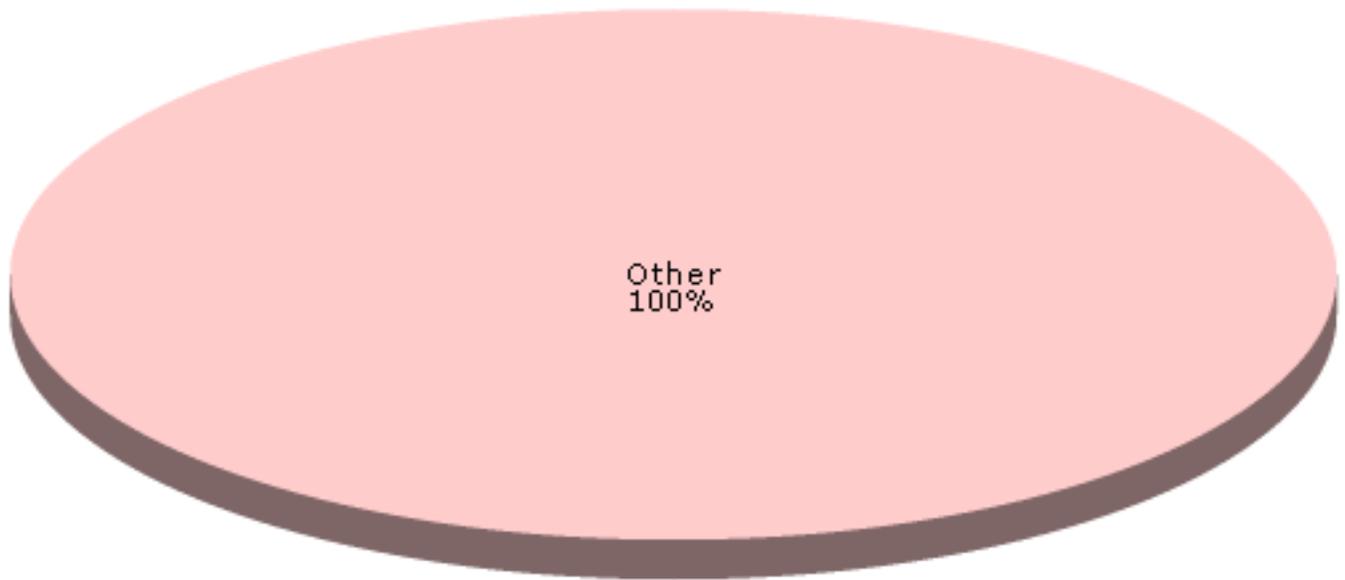
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.



2.3 Vulnerabilities by Class

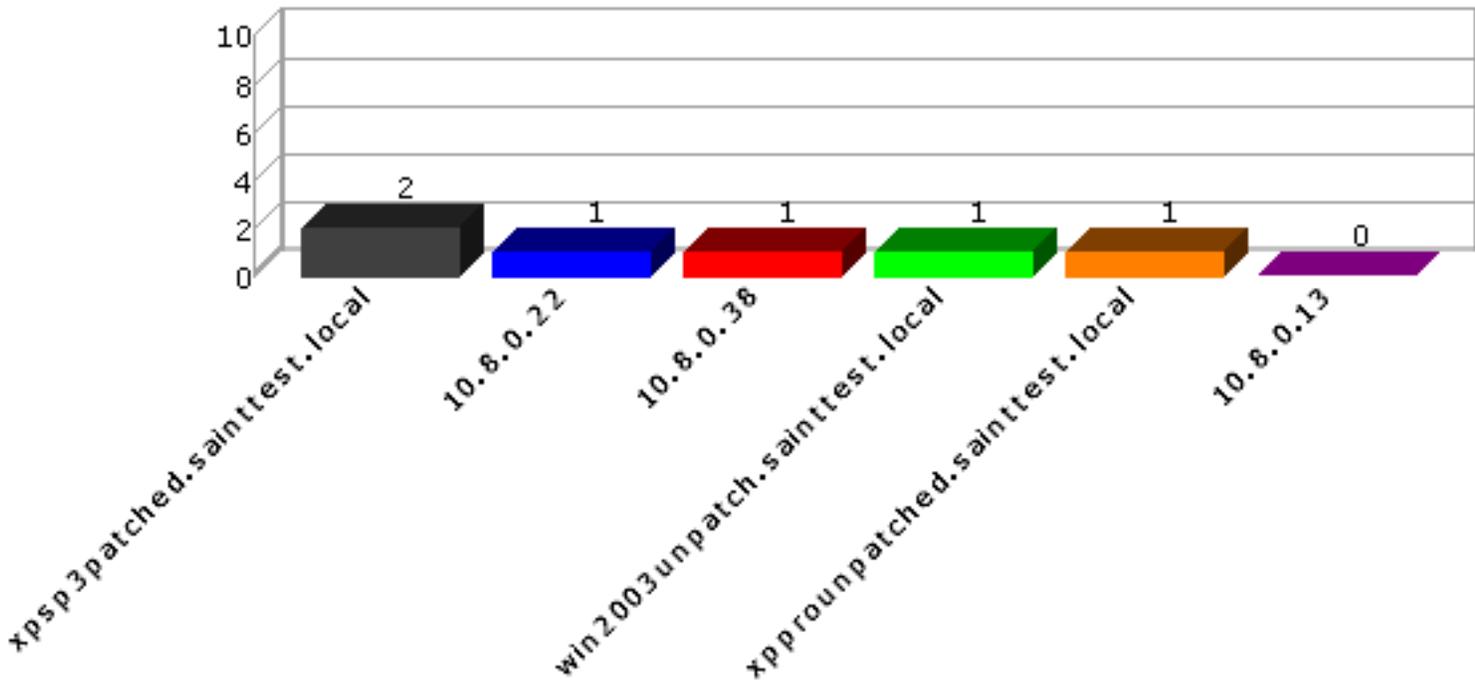
This section shows the number of vulnerabilities detected in each vulnerability class.





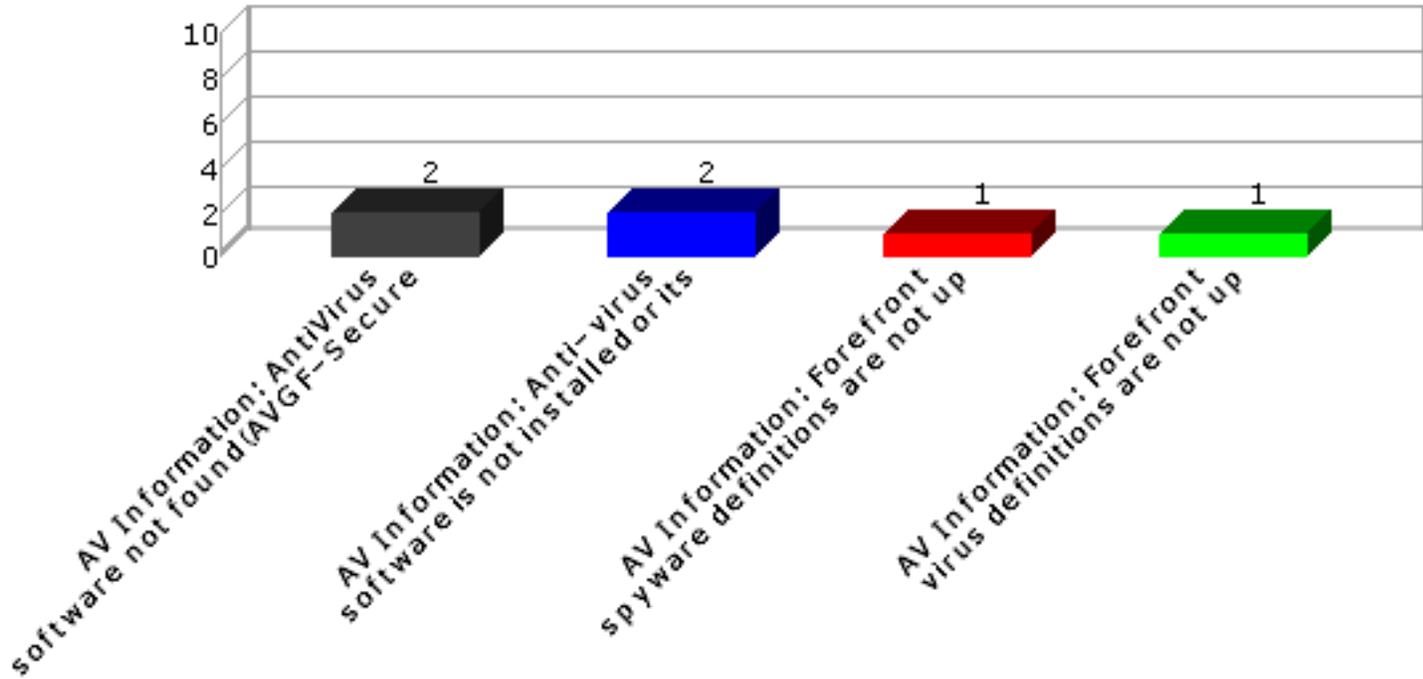
2.4 Top 10 Vulnerable Hosts

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



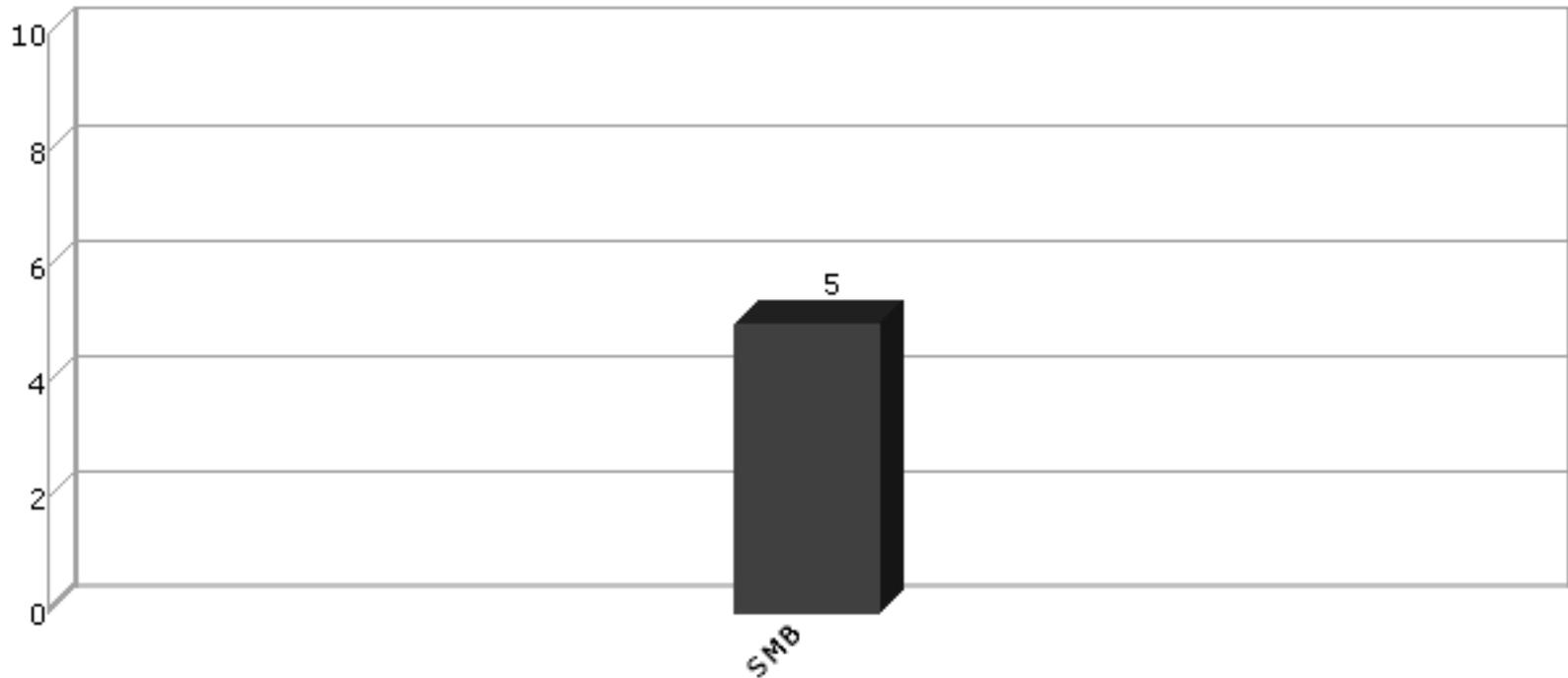
2.5 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, and the number of occurrences.



2.6 Top 10 Services

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



3 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
win2003unpatch.sainttest.local		10.8.0.11	Windows	0	0	1
10.8.0.13		10.8.0.13		0	0	0
xpprounpatched.sainttest.local		10.8.0.14	Windows	0	0	1
10.8.0.22		10.8.0.22	Windows	0	0	1
10.8.0.38		10.8.0.38	Windows	0	0	1
xpsp3patched.sainttest.local		10.8.0.104	Windows	0	0	2

3.2 Vulnerability List

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

Host Name	Port	Severity	Vulnerability / Service	Class	CVE	Max. CVSSv2 Base Score
win2003unpatch.sainttest.local	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
win2003unpatch.sainttest.local	139 /tcp	service	SMB			
10.8.0.13			nothing to report			
xpprounpatched.sainttest.local	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
xpprounpatched.sainttest.local	139 /tcp	service	SMB			
10.8.0.22	139 /tcp	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)	Other		2.6
10.8.0.22	139 /tcp	service	SMB			
10.8.0.22	139 /tcp	info	OS=[Windows Server 2012 R2 Standard 9600] Server=[Windows Server 2012 R2 Standard 6.3]			
10.8.0.38	139 /tcp	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)	Other		2.6
10.8.0.38	139 /tcp	service	SMB			
10.8.0.38	139 /tcp	info	OS=[Windows 7 Professional 7601 Service Pack 1] Server=[Windows 7 Professional 6.1]			
xpsp3patched.sainttest.local	139 /tcp	potential	AV Information: Forefront spyware definitions are not up to date	Other		2.6
xpsp3patched.sainttest.local	139 /tcp	potential	AV Information: Forefront virus definitions are not up to date	Other		2.6

xpsp3patched.sainttest.local	139	service	SMB
	/tcp		
xpsp3patched.sainttest.local	139	info	OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
	/tcp		

4 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 win2003unpatch.sainttest.local

IP Address: 10.8.0.11

Host type: Windows

Scan time: Dec 14 17:21:12 2015

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios
no registry access

SMB

Severity: Service

Technical Details

\131\000\000\001\143

4.2 10.8.0.13

IP Address: 10.8.0.13
Scan time: Dec 14 17:20:35 2015

nothing to report

4.3 xpprounpatched.sainttest.local

IP Address: 10.8.0.14 **Host type:** Windows
Scan time: Dec 14 17:21:12 2015

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios
no registry access

SMB

Severity: Service

Technical Details

\131\000\000\001\143

4.4 10.8.0.22

IP Address: 10.8.0.22 **Host type:** Windows
Scan time: Dec 14 17:21:12 2015

AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios
SAINT currently checks for AVG, F-Secure, Forefront, McAfee, Symantec, and TrendMicro AV software; none were detected

SMB

Severity: Service

Technical Details

\131\000\000\001\143

4.5 10.8.0.38

IP Address: 10.8.0.38

Host type: Windows

Scan time: Dec 14 17:21:12 2015

AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios

SAINT currently checks for AVG, F-Secure, Forefront, McAfee, Symantec, and TrendMicro AV software; none were detected

SMB

Severity: Service

Technical Details

\\131\000\000\001\143

4.6 xpsp3patched.sainttest.local

IP Address: 10.8.0.104

Host type: Windows

Scan time: Dec 14 17:21:12 2015

AV Information: Forefront spyware definitions are not up to date

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios

Virus definitions date is 2015-04-04

AV Information: Forefront virus definitions are not up to date

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see [Virus Bulletin](#).

Technical Details

Service: netbios

Virus definitions date is 2015-04-04

SMB

Severity: Service

Technical Details

\131\000\000\001\143

Scan Session: Antivirus status scan; Scan Policy: Anti-virus Information; Scan Data Set: 14 December 2015 17:21

Copyright 2001-2015 SAINT Corporation. All rights reserved.