SAINTwriter Assessment Report

Report Generated: June 20, 2019

1 Introduction

On May 15, 2019, at 1:06 AM, a PCI assessment was conducted using the SAINT 9.5.21 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, zero areas of concern, and one potential problem. The hosts and problems detected are discussed in greater detail in the following sections.

2 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.

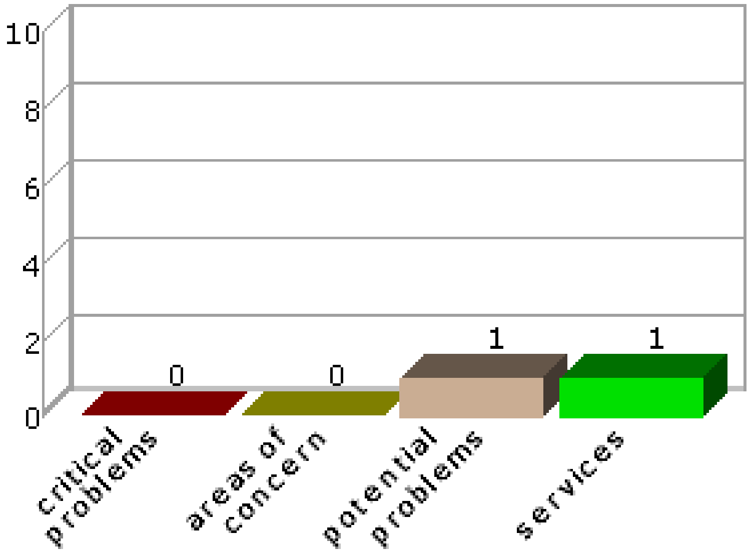
POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

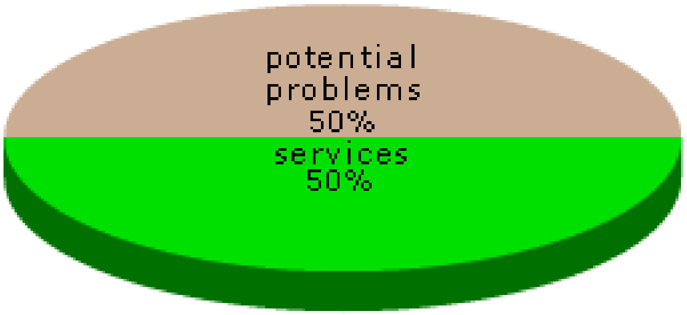
SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

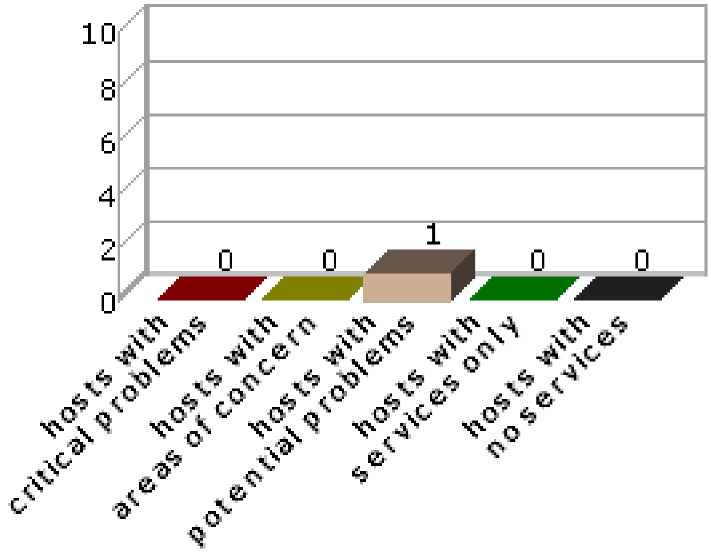
This section shows the overall number of vulnerabilities and services detected at each severity level.

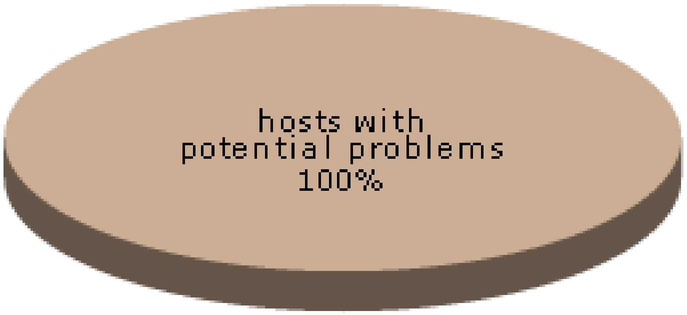




2.2 Hosts by Severity

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.

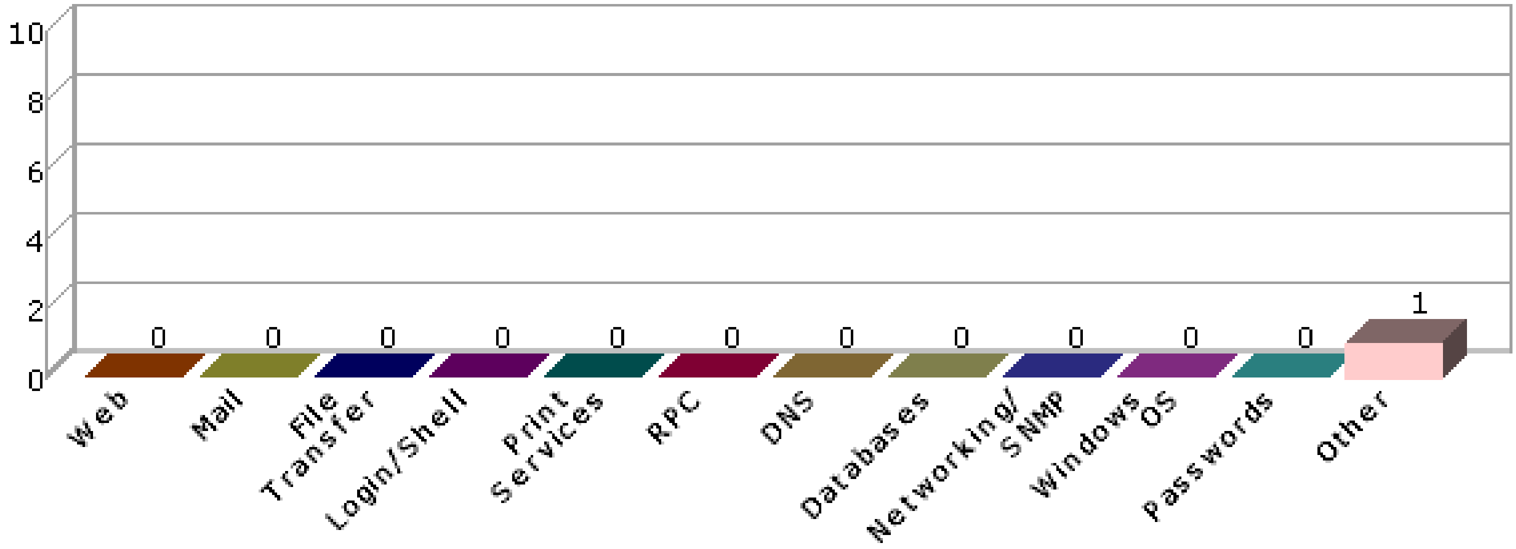


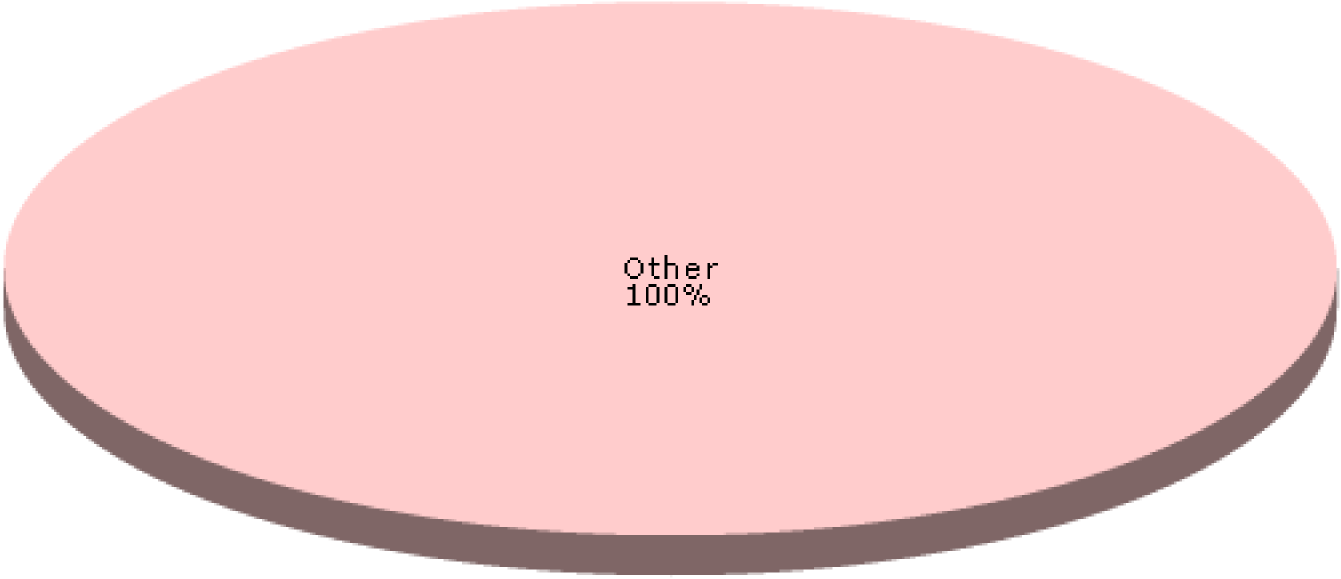


2.3 Vulnerabilities by Class

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

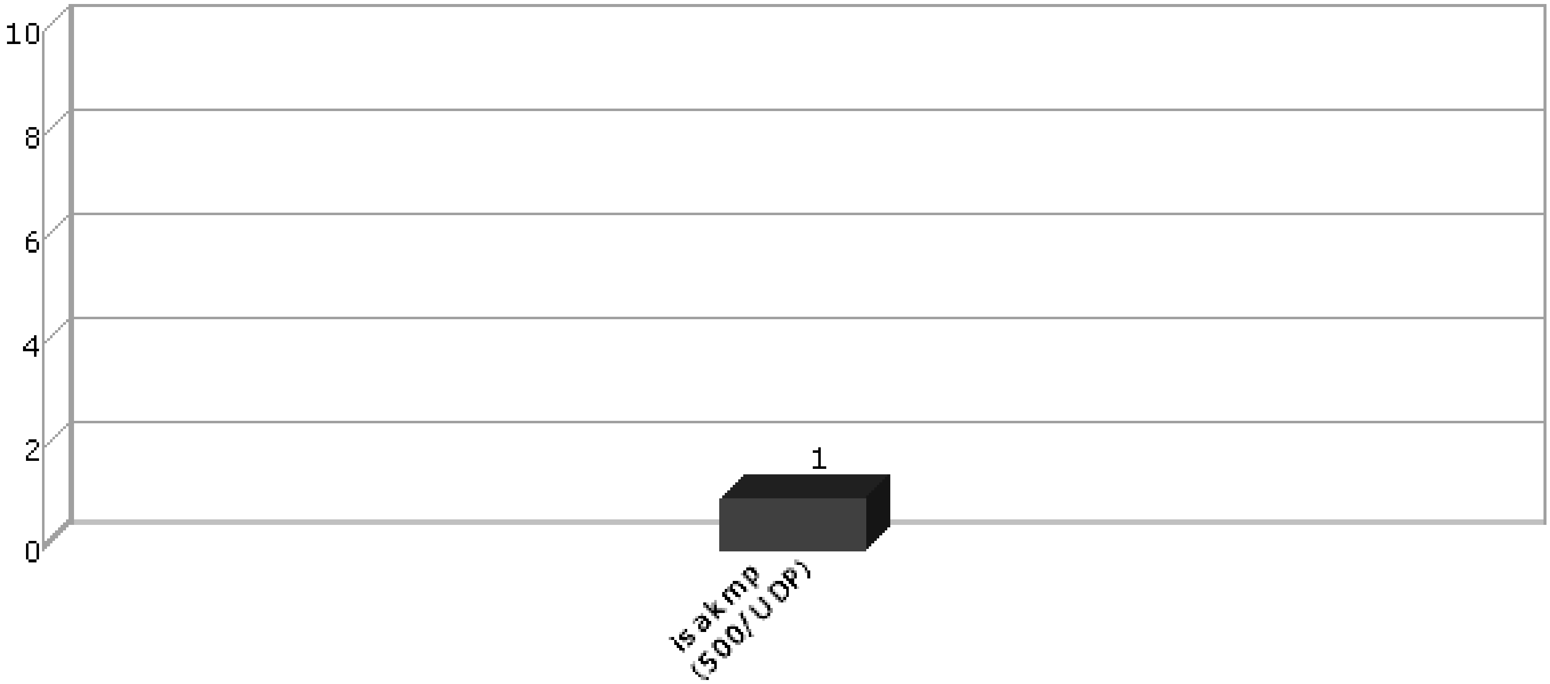
Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or 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 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
67.xxx.xx.xx		67.xxx.xx.xx		0	0	1

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?
67.xxx.xx.xx	potential	scan may be blocked	Other		no
67.xxx.xx.xx	service	isakmp (500/UDP)			no

4 Details

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

4.1 67.xxx.xx.xx

IP Address: 67.xxx.xx.xx
Scan time: May 15 01:06:18 2019

scan may be blocked

Severity: Potential Problem

Impact

The scan results may be inconclusive.

Resolution

Configure the firewall to permit at least the same level of access from the scanner as is permitted from the Internet in general.

References

See pages 14-15 of the PCI DSS ASV Program Guide for more information on handling interference during compliance scanning.

Technical Details

Service: 443:TCP
Connections to port(s) 443 are closed or filtered from the scanner but open from the Internet

isakmp (500/UDP)

Severity: Service

Technical Details

Copyright 2001-2019 SAINT Corporation. All rights reserved.

ASV Scan Report Executive Summary

Report Generated: June 20, 2019

Part 1. Scan Information

Scan Customer Company: Lundberg & Associates, PC	**ASV Company:**
Date scan was completed: May 15, 2019	**Scan expiration date:** August 13, 2019

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
67.xxx.xx.xx	FAIL

Part 3a. Vulnerabilities Noted for each Component

Component:Port	Vulnerability / Service	CVE	PCI Severity	CVSSv2 Base Score	PCI Compliant?	Exceptions, False positives, or Compensating Controls Noted by the ASV for this Vulnerability
67.xxx.xx.xx:443	scan may be blocked		low	2.6	FAIL	Scan results are inconclusive due to IPS

Consolidated Solution/Correction Plan for above Component: Make configuration changes for static block. See the Resolution section of the PCI Detail report for further instructions on correcting the above problems.

Part 3b. Special Notes by Component

Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed.
67.xxx.xx.xx	Remote access ports: 500 (isakmp)	Remote Access Software	

Part 3c. Special Notes - Full Text

Remote access ports

Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

- 67.xxx.xx.xx

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

- 67.xxx.xx.xx

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

No out-of-scope components were found.

Scan Session: mID269233; Scan Policy: PCI; Scan Data Set: 15 May 2019 01:06

Copyright 2001-2019 SAINT Corporation. All rights reserved.