

## Scan Results

01/24/2023

The scan was started on January 24, 2023 at 10:13 pm GMT and took 00:19:06 to complete. The scan was run against the following IP addresses:

# Not a certified PCI report

### IP/DNS Scanned

64.41.200.245-64.41.200.247

The scan option profile used includes:

#### Scan Settings

Scanned TCP Ports	Full
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication	Disabled
SSH Authentication	Disabled
Oracle Authentication	Disabled
SNMP Authentication	Disabled
Perform 3-way Handshake	Off
Overall Performance	N/A
Hosts to Scan in Parallel-External Scanner	N/A
Hosts to Scan in Parallel-Scanner Appliances	N/A
Processes to Run in Parallel-Total	N/A
Processes to Run in Parallel-HTTP	N/A
Packet (Burst) Delay	N/A

#### Advanced Settings

Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Ignore RST packets	Off
Ignore firewall-generated SYN-ACK packets	Off
ACK/SYN-ACK packets during discovery	Send

## Report Summary

Company:	Training-Qualys_bpallo@blue-aegis.com
User:	Ben Pallotti
Template Title:	Scan Results
Active Hosts:	2
Total Hosts:	3
Scan Type:	On Demand
Scan Status:	Finished
Scan Title:	External PCI Scan using VM
Scan Date:	01/24/2023 at 22:13:11
Reference:	scan/1674598391.16006
Scanner Appliance:	64.39.98.39 (Scanner 12.12.48-1, Vulnerability Signatures 2.5.684-2)
Duration:	00:19:06
Options:	Payment Card Industry (PCI) Options
Target:	64.41.200.245-64.41.200.247

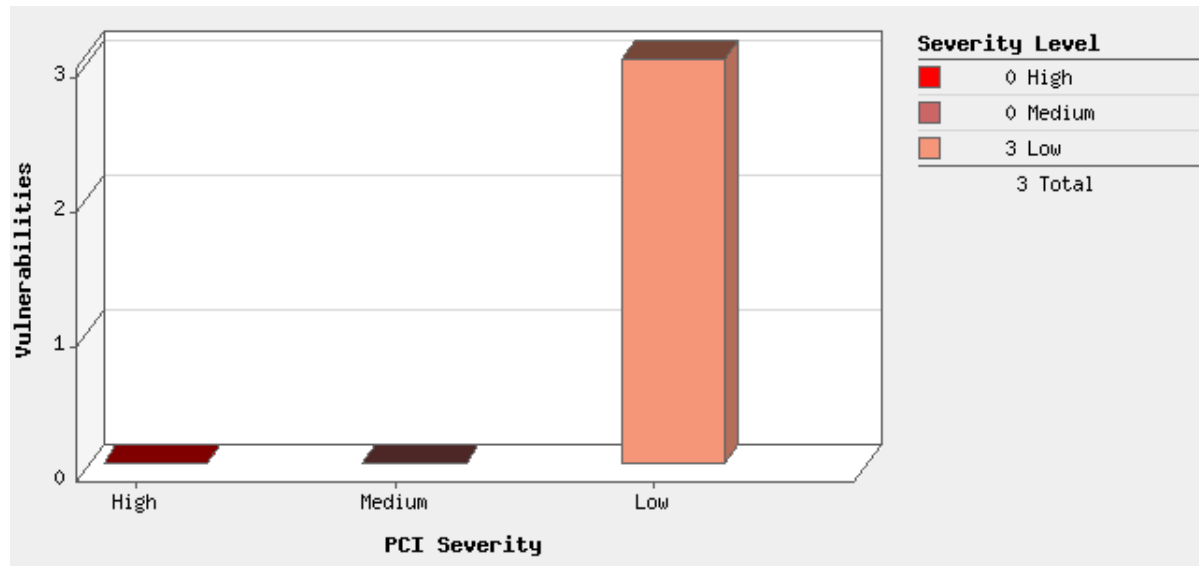
## Summary of Vulnerabilities

Vulnerabilities Total	36	Average Security Risk	<div><div></div><div></div><div></div><div></div><div></div></div>	1.5
-----------------------	----	-----------------------	--	-----

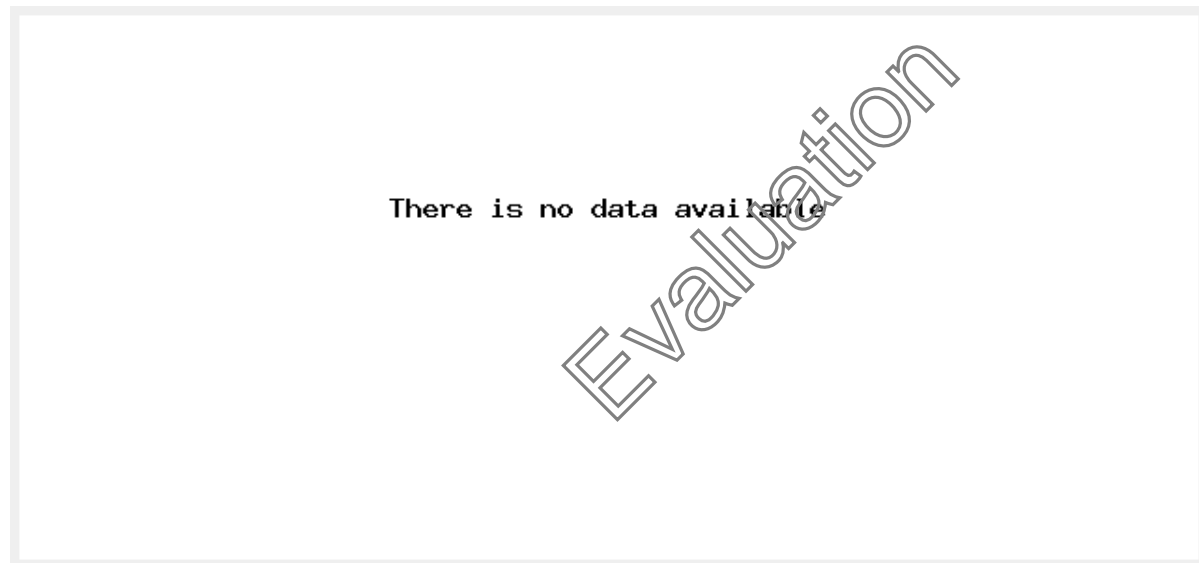
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	1	0	4	5
1	2	0	28	30
Total	3	0	33	36

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	3	0	3
Total	3	0	3

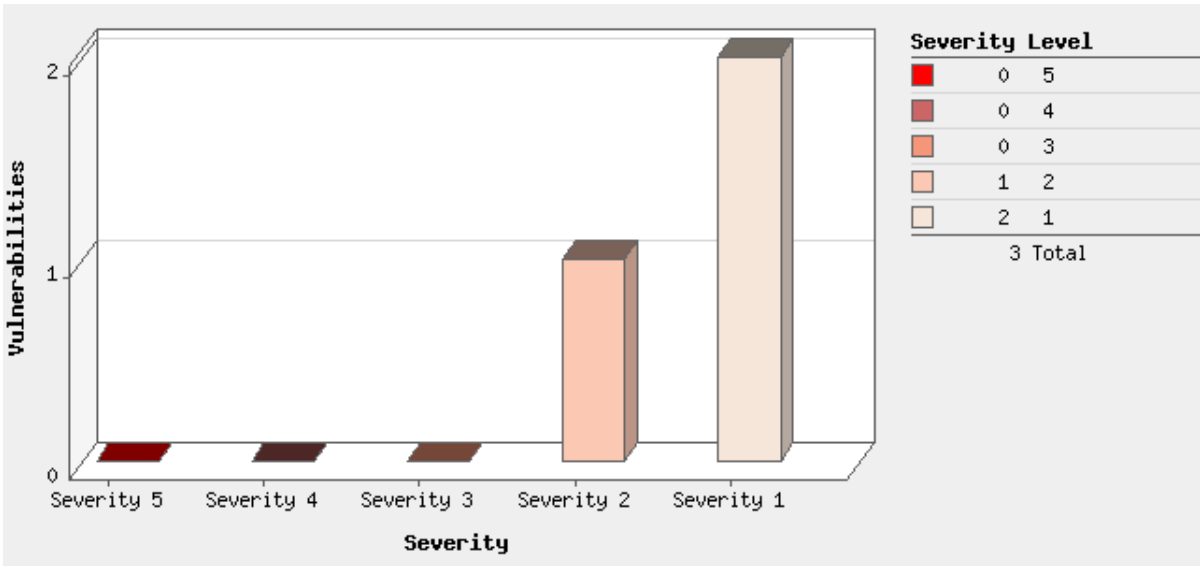
## Vulnerabilities by PCI Severity



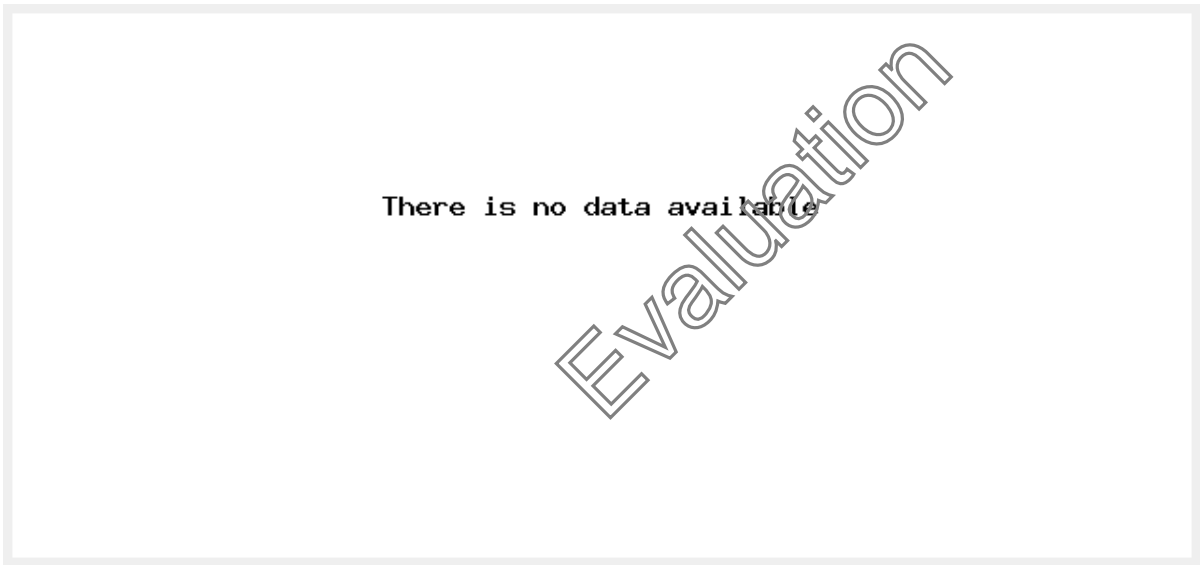
## Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity



## Detailed Results

64.41.200.245 (demo15.s02.sjc01.qualys.com,-)

Vulnerabilities Total

9

Security Risk

1.0

Compliance Status

PASS

### Vulnerabilities (1)

#### ICMP Timestamp Request

##### PCI COMPLIANCE STATUS

PCI Severity:

LOW

PASS

The QID adheres to the PCI requirements based on the CVSS basescore.  
The vulnerability is purely a denial-of-service (DoS) vulnerability.

##### VULNERABILITY DETAILS

CVSS Base Score: 2.1 AV:/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 1.9 E:F/RL:W/RC:C

Severity: 1

QID: 82003

Category: TCP/IP

CVE ID: CVE-1999-0524

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/29/2009

##### THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. Its principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

##### IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

##### SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

##### RESULT:

Timestamp of host (network byte ordering): 22:26:23 GMT


### Information Gathered (8)

#### DNS Host Name

## PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 6  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/04/2018

#### THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

#### RESULT:


IP address	Host name
64.41.200.245	demo15.s02.sjc01.qualys.com

## Traceroute

## PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 45006  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/09/2003

#### THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

#### RESULT:


Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.1	1.06ms	ICMP	
2	4.15.10.202	0.62ms	ICMP	
3	4.15.10.201	1.10ms	ICMP	
4	***	0.00ms	Other	80
5	4.30.195.50	10.23ms	ICMP	
6	141.101.72.32	10.30ms	ICMP	
7	172.69.32.109	9.75ms	ICMP	
8	172.69.32.109	9.75ms	ICMP	
9	172.70.209.136	9.85ms	ICMP	
10	***	0.00ms	Other	80
11	64.41.200.245	22.71ms	ICMP	

## Target Network Information

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 45004  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 08/15/2013

#### THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

#### IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

#### RESULT:


The network handle is: CENTURYLINK-LEGACY-SAVVIS-BLK220  
Network description:  
CenturyLink Communications, LLC

## Internet Service Provider

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 45005  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 09/27/2013

#### THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

#### IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.


#### RESULT:

## Host Names Found

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 45039  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 08/27/2020

#### THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

#### RESULT:


Host Name	Source
demo15.s02.sjc01.qualys.com	FQDN

## Host Scan Time - Scanner

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 45038  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 09/15/2022

#### THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

#### RESULT:



Scan duration: 503 seconds

Start time: Tue, Jan 24 2023, 22:15:06 GMT


End time: Tue, Jan 24 2023, 22:23:29 GMT

## ICMP Replies Received

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1 

QID: 82040

Category: TCP/IP

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 01/16/2003

#### THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)  
Timestamp Request (to trigger Timestamp Reply)  
Address Mask Request (to trigger Address Mask Reply)  
UDP Packet (to trigger Port Unreachable Reply)  
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

#### RESULT:


ICMP Reply Type	Triggered By	Additional Information
Unreachable (type=3 code=3)	UDP Port 9872	Port Unreachable
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 56266	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1812	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1041	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 500	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	22:26:23 GMT
Unreachable (type=3 code=3)	UDP Port 555	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1031	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 43831	Port Unreachable

## Firewall Detected

## PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 34011  
Category: Firewall  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 04/22/2019

#### THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

#### RESULT:

Some of the ports filtered by the firewall are: 22, 80.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

22,80,2222

64.41.200.247 (trn-win7.trn.qualys.com,TRN-WIN7)

Windows 2008 R2/7

Vulnerabilities Total

27

Security Risk

2.0

Compliance Status

**PASS**

### Vulnerabilities (2)


#### NetBIOS Name Accessible

## PCI COMPLIANCE STATUS

PCI Severity:  LOW

**PASS**

### VULNERABILITY DETAILS

CVSS Base Score: 0  
CVSS Temporal Score: 0  
Severity: 2   
QID: 70000  
Category: SMB / NETBIOS  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 04/28/2009

#### THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

#### IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

**SOLUTION:**

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

**RESULT:**

TRN-WIN7

## ICMP Timestamp Request

**PCI COMPLIANCE STATUS**

PCI Severity:

■ **LOW**

**PASS**

The QID adheres to the PCI requirements based on the CVSS basescore.  
The vulnerability is purely a denial-of-service (DoS) vulnerability.

**VULNERABILITY DETAILS**

CVSS Base Score: **2.1** AV:/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: **1.9** E:F/RL:W/RC:C

Severity: **1** ■

QID: 82003

Category: TCP/IP

CVE ID: [CVE-1999-0524](#)

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/29/2009

**THREAT:**

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

**IMPACT:**

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

**SOLUTION:**

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

**RESULT:**

Timestamp of host (host byte ordering): 21:50:16 GMT


## Information Gathered (25)

### NetBIOS Bindings Information

## PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 3   
QID: 70004  
Category: SMB / NETBIOS  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/09/2005

#### THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

#### IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

#### SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be accessible to external networks, and should be firewalled.

#### RESULT:


Name	Service	NetBIOS Suffix
TRN-WIN7	Workstation Service	0x0
TRN	Domain Name	0x0
TRN-WIN7	File Server Service	0x20
TRN	Browser Service Elections	0x1e

## Operating System Detected

## PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 2   
QID: 45017  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/16/2023

#### THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

**IMPACT:**

Not applicable.

**SOLUTION:**

Not applicable.

**RESULT:**


Operating System	Technique	ID
Windows 2008 R2/7	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3041:135

## Windows Registry Pipe Access Level

**PCI COMPLIANCE STATUS**

**PASS**

**VULNERABILITY DETAILS**

Severity: **2**   
QID: 90194  
Category: Windows  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/16/2005

**THREAT:**

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

**IMPACT:**

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

**SOLUTION:**

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

**RESULT:**


Access to Remote Registry Service is denied, error: 0x0

## Open DCE-RPC / MS-RPC Services List

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 2   
QID: 70022  
Category: SMB / NETBIOS  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/22/2019

#### THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

#### SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

#### RESULT:


Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc
Microsoft Security Account Manager	1.0	49155			\pipe\lsass
Microsoft Service Control Service	2.0	53404			
Microsoft Spool Subsystem	1.0	53405			
Microsoft Task Scheduler	1.0				\PIPE\atsvc
WinHttp Auto-Proxy Service	5.1				\PIPE\W32TIME_ALT
(Unknown Service)	1.0	49152			\PIPE\InitShutdown
(Unknown Service)	1.0				\PIPE\InitShutdown
Security Center	1.0	49153			\pipe\eventlog
DHCP Client LRPC Endpoint	1.0	49153			\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0	49153			\pipe\eventlog
NRP server endpoint	1.0	49153			\pipe\eventlog
Event log TCPIP	1.0	49153			\pipe\eventlog
Impl friendly name	1.0	49154			\PIPE\srvsvc, \PIPE\atsvc
(Unknown Service)	1.0	49154			\PIPE\srvsvc, \PIPE\atsvc
XactSrv service	1.0	49154			\PIPE\atsvc
IP Transition Configuration endpoint	1.0	49154			\PIPE\atsvc
IKE/Authip API	1.0	49154			\PIPE\atsvc
(Unknown Service)	1.0	49154			\PIPE\atsvc
Remote Fw APIs	1.0	53405			
(Unknown Service)	1.0				\pipe\trkwks

## Host Uptime Based on TCP TimeStamp Option

### PCI COMPLIANCE STATUS

PASS

## VULNERABILITY DETAILS

Severity: 2   
QID: 82063  
Category: TCP/IP  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/29/2007

### THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

### RESULT:


Based on TCP timestamps obtained via port 135, the host's uptime is 487 days, 5 hours, and 1 minutes.  
The TCP timestamps from the host are in units of 10 milliseconds.

## DNS Host Name

### PCI COMPLIANCE STATUS

**PASS**

## VULNERABILITY DETAILS

Severity: 1   
QID: 6  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/04/2018

### THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

### RESULT:


IP address	Host name
64.41.200.247	demo17.s02.sjc01.qualys.com

## Traceroute

### PCI COMPLIANCE STATUS

**PASS**

## VULNERABILITY DETAILS

Severity: 1   
QID: 45006  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/09/2003

### THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

### RESULT:


Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.10	0.76ms	ICMP	
2	4.15.10.202	0.49ms	ICMP	
3	4.15.10.201	1.04ms	ICMP	
4	4.69.215.133	9.70ms	ICMP	
5	4.30.195.50	10.11ms	ICMP	
6	162.158.88.3	9.68ms	ICMP	
7	172.70.205.120	9.68ms	ICMP	
8	172.70.205.69	9.85ms	ICMP	
9	172.70.205.63	9.79ms	ICMP	
10	*.*.*	0.00ms	Other	80
11	64.41.200.247	24.42ms	UDP	80

## Target Network Information

### PCI COMPLIANCE STATUS

**PASS**

## VULNERABILITY DETAILS

Severity: 1   
QID: 45004  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 08/15/2013

### THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

### IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

### RESULT:




## Internet Service Provider

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 45005  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 09/27/2013

#### THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

#### IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

#### RESULT:


The ISP network handle is: CLOUDFLARENET  
ISP Network description:  
Cloudflare, Inc.

## SMB Version 1 Enabled

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 45261  
Category: Information gathering  
CVE ID: -  
Vendor Reference: [SMB v1](#)  
Bugtraq ID: -  
Last Update: 09/19/2019

#### THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.

The Windows host has SMBv1 protocol enabled for either :  
Client or

**IMPACT:**

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

**SOLUTION:**

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.


Refer to Microsoft KB article KB2696547 (<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>) for more details.

Workaround: Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

**RESULT:**

QID: 45261 detected on port 445 over TCP.  
SMBv1 is enabled.

**SMB Version 2 or 3 Enabled****PCI COMPLIANCE STATUS****PASS****VULNERABILITY DETAILS**

Severity: 1   
QID: 45262  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 11/22/2022

**THREAT:**

The Windows host has SMBv2 or SMBv3 protocol enabled.

**SOLUTION:**


For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows>).

**RESULT:**

QID: 45262 detected on port 445 over TCP.  
SMBv2 is enabled.

**Host Names Found****PCI COMPLIANCE STATUS****PASS**

## VULNERABILITY DETAILS

Severity: 1   
QID: 45039  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 08/27/2020

### THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

### RESULT:


Host Name	Source
trn-win7.trn.qualys.com	NTLM DNS
demo17.s02.sjc01.qualys.com	FQDN
TRN-WIN7	NTLM NetBIOS
TRN-WIN7	NetBIOS

## Host Scan Time - Scanner

### PCI COMPLIANCE STATUS

**PASS**

## VULNERABILITY DETAILS

Severity: 1   
QID: 45038  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 09/15/2022

### THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

### RESULT:

Scan duration: 1098 seconds

Start time: Tue, Jan 24 2023, 22:14:49 GMT


End time: Tue, Jan 24 2023, 22:33:07 GMT

## Scan Activity per Port

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 45426  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/24/2020

### THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

### RESULT:


Protocol	Port	Time
TCP	135	0:01:29
TCP	445	0:01:08
TCP	49152	0:05:06
TCP	49153	0:05:06
TCP	49154	0:05:06
TCP	49155	0:05:06
TCP	53404	0:05:06
TCP	53405	0:05:06
TCP	65529	0:13:54
UDP	123	0:00:19
UDP	137	0:00:56
UDP	138	0:00:07
UDP	500	0:00:12
UDP	1900	0:00:12

## ICMP Replies Received

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 82040  
Category: TCP/IP  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/16/2003

### THREAT:

### RESULT:


ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 13762	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2002	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1029	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	21:50:16 GMT
Unreachable (type=3 code=3)	UDP Port 19	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 12223	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9824	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 61466	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 32771	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1999	Port Unreachable

## NetBIOS Workgroup Name Detected

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
 QID: 82062  
 Category: TCP/IP  
 CVE ID: -  
 Vendor Reference: -  
 Bugtraq ID: -  
 Last Update: 06/02/2005

#### THREAT:

The NetBIOS workgroup or domain name for this system has been detected.

#### RESULT:


TRN

## NetBIOS Host Name

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
 QID: 82044  
 Category: TCP/IP  
 CVE ID: -  
 Vendor Reference: -  
 Bugtraq ID: -  
 Last Update: 01/21/2005

#### THREAT:

The NetBIOS host name of this computer has been detected.


#### RESULT:

## Degree of Randomness of TCP Initial Sequence Numbers

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1 

QID: 82045

Category: TCP/IP

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 11/19/2004

#### THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

#### RESULT:


Average change between subsequent TCP initial sequence numbers is 784052083 with a standard deviation of 829894492. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5108 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

## IP ID Values Randomness

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1 

QID: 82046

Category: TCP/IP

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 07/27/2006

#### THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

#### RESULT:


IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 4 7  
Duration: 30 milli seconds

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1   
QID: 82023  
Category: TCP/IP  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/15/2009

**THREAT:**  
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

**IMPACT:**  
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

**SOLUTION:**  
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

**RESULT:**


Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
53404	unknown	unknown	msrpc	
53405	unknown	unknown	msrpc	
65529	unknown	unknown	unknown	

Open UDP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1   
QID: 82004  
Category: TCP/IP  
CVE ID: -  
Vendor Reference: -

Bugtraq ID: -  
Last Update: 07/11/2005

#### THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

#### IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

#### SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

#### RESULT:


Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
500	isakmp	isakmp	unknown
1900	unknown	unknown	unknown

## File and Print Services Access Denied

#### PCI COMPLIANCE STATUS

**PASS**

#### VULNERABILITY DETAILS

Severity: 1   
QID: 70038  
Category: SMB / NETBIOS  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/06/2005

#### THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

#### IMPACT:

Vulnerabilities that require authenticated access may not be reported.

#### SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

#### RESULT:

No results available




## Windows Authentication Method

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 70028  
Category: SMB / NETBIOS  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 12/09/2008

#### THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.

The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

#### RESULT:


User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session; no valid login credentials provided or found
CIFS Signing	default

## Network Adapter MAC Address

### PCI COMPLIANCE STATUS

PASS

### VULNERABILITY DETAILS

Severity: 1   
QID: 43007  
Category: Hardware  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/18/2020

#### THREAT:

It is possible to obtain the MAC address information of the network adapters on the target system. Various sources such as SNMP and NetBIOS provide such information. This vulnerability test attempts to gather and report on this information in a table format.

#### RESULT:


Method	MAC Address	Vendor
NBTSTAT	00:50:56:B2:71:56	VMWARE, INC.

## Firewall Detected

### PCI COMPLIANCE STATUS

**PASS**

### VULNERABILITY DETAILS

Severity: 1   
QID: 34011  
Category: Firewall  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 04/22/2019

#### THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

#### RESULT:

Some of the ports filtered by the firewall are: 22, 80.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

22,80,2222

## Appendices

### Hosts Scanned

64.41.200.245, 64.41.200.247

### Hosts Not Alive

64.41.200.246

### Option Profile

#### Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off
Overall Performance:	N/A
Hosts to Scan in Parallel-External Scanner:	N/A
Hosts to Scan in Parallel-Scanner Appliances:	N/A
Processes to Run in Parallel-Total:	N/A

Processes to Run in Parallel-HTTP:	N/A
Packet (Burst) Delay:	N/A

## Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

## Report Legend

### Payment Card Industry (PCI) Status






The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.




A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

### Vulnerability Levels






A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.




Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
 LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
 MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

### Potential Vulnerability Levels




A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
 LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
 MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

#### Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.