Payment Card Industry (PCI) Technical Report

01/02/2023

ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				**A2. Approved Scanning Vendor Information**			
Company:	Qualys_Training_tenley@wildun.ca			Company:	Qualys		
Contact Name:	Tenley Wiltshire	Job Title:		Contact Name:	-	Job Title:	-
Telephone:		Email:	tenley@wildun.ca	Telephone:	-	Email:	-
Business Address:	919 E Hillsdale Blvd,			Business Address:	919 E Hillsdale Blvd, 4th Floor		
City:	Foster City, CA 94404	State/Province:	California	City:	Foster City	State/Province:	California
ZIP/postal code:		Country:	United States of America	ZIP/postal code:	94404	Country:	United States of America
URL:				URL:	http://www.qualys.com/		

A3. Scan Status			
Date scan completed	12/25/2022	Scan expiration date (90 days from date scan completed)	03/25/2023
Compliance Status	FAIL	Scan report type	Full scan
Number of unique in-scope components scanned			2
Number of identified failing vulnerabilities			3
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

A.4 Scan Customer Attestation

Qualys_Training_tenley@wildun.ca attests on 01/02/2023 at 15:11:54 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/ rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions - including compensating controls if applicable- is accurate and complete.
Qualys_Training_tenley@wildun.ca also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Qualys under certificate number 3728-01-17, according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.
Qualys attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by N/A

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	Qualys_Training_tenley@wildun.ca	ASV Company:	Qualys
Date scan was completed:	12/25/2022	Scan expiration date:	03/25/2023

Part 2. Component Compliance Summary

64.41.200.245, demo15.s02.sjc01.qualys.com	FAIL
64.41.200.247, trn-win7.trn.qualys.com	PASS

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
64.41.200.245, demo15.s02.sjc01.qualys.com port 22/tcp	38739 - Deprecated SSH Cryptographic Settings	■ MED	6.4	FAIL	The vulnerability is not included in the NVD. ASV Score = 6.4
64.41.200.245, demo15.s02.sjc01.qualys.com	45002 - Global User List Found Using Other QIDS	■ MED	5	FAIL	Automatic Failure: Built-in or default accounts and passwords The vulnerability is not included in the NVD.
64.41.200.245, demo15.s02.sjc01.qualys.com port 22/tcp	38737 - OpenSSH User Enumeration CVE-2018-15473	■ MED	5	FAIL	
64.41.200.245, demo15.s02.sjc01.qualys.com	82003 - ICMP Timestamp Request CVE-1999-0524	■ LOW	2.1	PASS	The vulnerability is purely a denial-of-service (DoS) vulnerability.
	Consolidated Solution/Correction Plan for 64.41.200.245 **ASV Comment:** Please update OpenSSH to the latest versions.Change built-in or default accounts and passwords.				
64.41.200.247, trn-win7.trn.qualys.com	82003 - ICMP Timestamp Request CVE-1999-0524	■ LOW	2.1	PASS	The vulnerability is purely a denial-of-service (DoS) vulnerability.
64.41.200.247, trn-win7.trn.qualys.com	70000 - NetBIOS Name Accessible	■ LOW	0	PASS	The vulnerability is not included in the NVD. ASV Score = 0

Part 3b. Special Notes by Component

Component	Special Note	Item Noted (remote access software, POS software, etc.)	Scan customer's description of actions taken and declaration that software is either implemented securely or removed
64.41.200.245	Remote Access	42017 - Remote Access or Management Service Detected (SSH:port 22/TCP)	No - Student Test
64.41.200.247	Unknown services	82023 - Open TCP Services List (TCP/IP)	No - Student Test
64.41.200.247	Unknown services	82004 - Open UDP Services List (TCP/IP)	No - Student Test

Part 3c. Special Notes Full Text

Note
Remote Access Note to Scan Customer : Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.
Unknown services Note to Scan Customer : Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implememted, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.
64.41.200.245-64.41.200.247

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

IP Addresses/ranges/subnets, domains, URLs, etc.
64.41.200.245, demo15.s02.sjc01.qualys.com
64.41.200.247, trn-win7.trn.qualys.com

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

IP Addresses/ranges/subnets, domains, URLs, etc.
IP Addresses/Ranges : - (not active) Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.

Report Summary

Company:	Qualys_Training_tenley@wildun.ca
Hosts in Account:	3 IP
Hosts Active:	2
Hosts Scanned:	3
Scan Date:	12/25/2022 at 14:36:18 GMT
Report Date:	01/02/2023 at 15:11:53 GMT
Report Title:	Q@ PCI Report
Template Title:	Payment Card Industry (PCI) Technical Report

Summary of Vulnerabilities

Vulnerabilities Total	46	Average Security Risk	🟥🟥🟥⬜⬜ 2.5

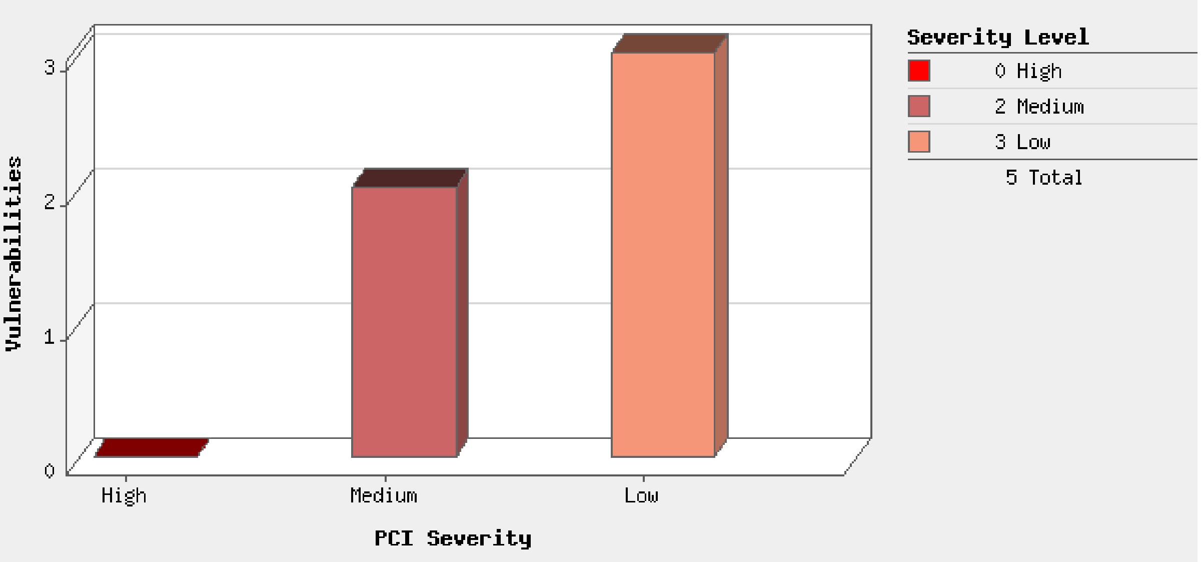
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	0	2	4
2	1	1	6	8
1	2	0	32	34
Total	5	1	40	46

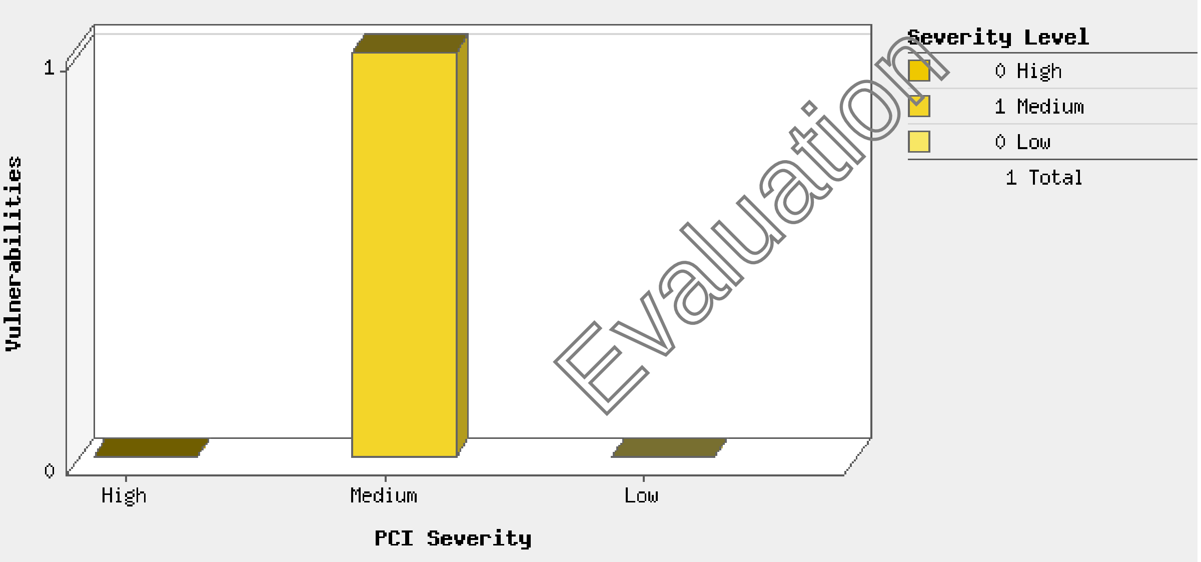
by PCI Severity

PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	2	1	3
Low	3	0	3
Total	5	1	6

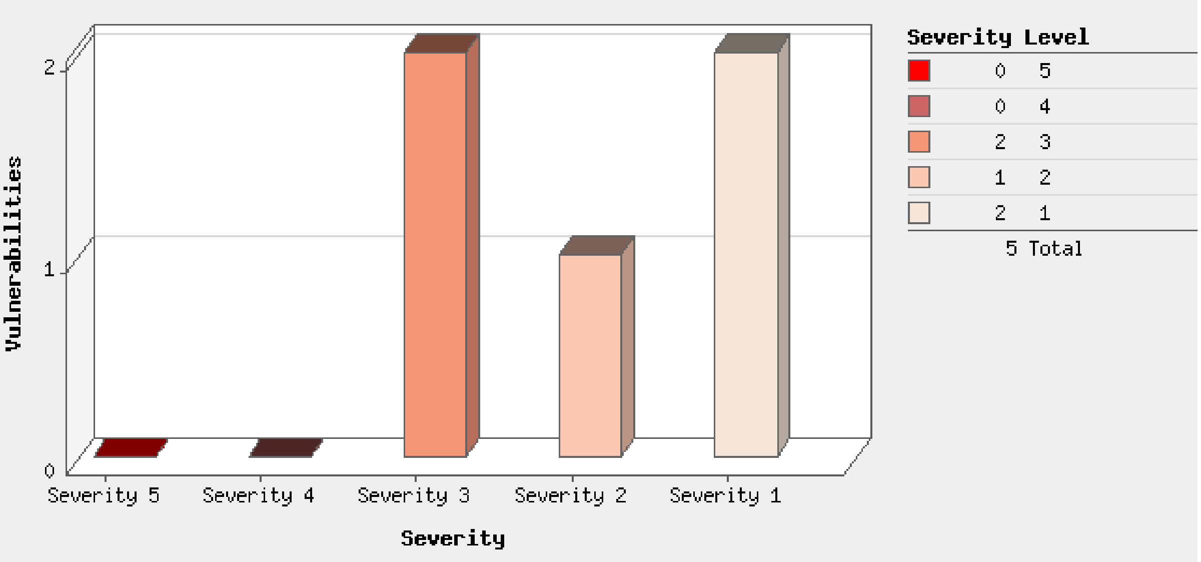
Vulnerabilities by PCI Severity



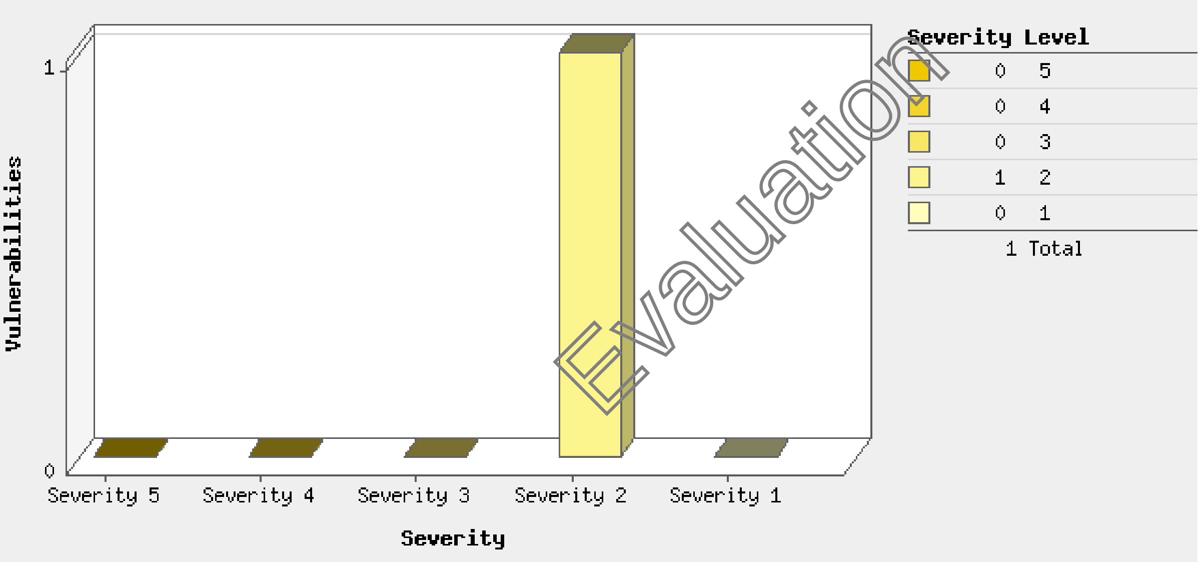
Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity



Detailed Results

64.41.200.245 (demo15.s02.sjc01.qualys.com,-) Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / H...

Vulnerabilities Total	20	Security Risk	🟥🟥🟥□□ 3.0

Vulnerabilities (3)

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 (network byte ordering): 14:49:17 GMT

Deprecated SSH Cryptographic Settings port 22/tcp

PCI COMPLIANCE STATUS

PCI Severity:	🟥 MED

FAIL The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**6.4**	AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	**4.7**	E:U/RL:W/RC:UC
Severity:	**3**	🟥🟥🟥□□
QID:	38739	
Category:	General remote services	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	05/26/2021	

THREAT:
The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.

The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:
A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:
Avoid using deprecated cryptographic settings.

Use best practices when configuring SSH.

Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) (https://csrc.nist.gov/publications/detail/nistir/7966/final) .

Settings currently considered deprecated:

Ciphers using CFB of OFB
Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM
RC4 cipher (arcfour, arcfour128, arcfour256)
The RC4 cipher has a cryptographic bias and is no longer considered secure
Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)
Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)
Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)
DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks
Key exchange algorithm "rsa1024sha1"
Very uncommon, and deprecated because of the short RSA key size
MAC algorithm "umac-32"
Very uncommon, and deprecated because of the very short MAC length
Cipher "none"
This is available only in SSHv1

RESULT:

Type	Name
key exchange	diffie-hellman-group1-sha1
cipher	arcfour256
cipher	arcfour128
cipher	3des-cbc
cipher	blowfish-cbc

cipher	cast128-cbc
cipher	arcfour

OpenSSH User Enumeration

port 22/tcp

PCI COMPLIANCE STATUS

PCI Severity: ■ MED

FAIL

The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**5**	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.1**	E:F/RL:OF/RC:C
Severity:	**3**	🟥🟥🟥□□
QID:	38737	
Category:	General remote services	
CVE ID:	CVE-2018-15473	
Vendor Reference:	-	
Bugtraq ID:	105140	
Last Update:	01/03/2019	

THREAT:
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.

In order for this vulnerability to be detected the "Password Brute Forcing" setting in the scan option profile needs to have a "System" value of "Standard" or higher.

IMPACT:
A remote attacker could check is a specific user account existed on the target server.

SOLUTION:
Upgrade to OpenSSH 7.8/7.8p1 or the latest version of openssh package for your operating system.

OpenSSH is available for download from OpenSSH's Web site (http://www.openssh.org/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8/7.8p1: OpenSSH (https://www.openssh.com/releasenotes.html)

RESULT:

```
root adm bin daemon ftp games halt lp mail nobody operator root shutdown sync
```

Potential Vulnerabilities (1)

Global User List Found Using Other QIDS

PCI COMPLIANCE STATUS

PCI Severity: MED

FAIL

The QID adheres to the PCI requirements based on the CVSS basescore.
Automatic Failure: Built-in or default accounts and passwords

VULNERABILITY DETAILS

CVSS Base Score:	**5**	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.8**	E:H/RL:W/RC:C
Severity:	**2**	
QID:	45002	
Category:	Information gathering	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	11/23/2021	

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
root	38737
adm	38737
bin	38737
daemon	38737
ftp	38737
games	38737
halt	38737
lp	38737
mail	38737
nobody	38737
operator	38737
shutdown	38737
sync	38737

Information Gathered (16)

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

SSH Banner

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/30/2020

THREAT:
Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:
The QID checks for SSH in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

RESULT:

```
SSH-2.0-OpenSSH_6.6.1
```

SSH daemon information retrieving

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/04/2018

THREAT:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentification methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc, rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc, rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96
Supported authentification methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:
Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:
SSH version 2 is preferred over SSH version 1.

RESULT:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa, ecdsa-sha2-nistp256, ssh-ed25519
Supported decryption ciphers for SSH2	aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, aes192-cbc, aes256-cbc, arcfour, rijndael-cbc@lysator.liu.se
Supported encryption ciphers for SSH2	aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, aes192-cbc, aes256-cbc, arcfour, rijndael-cbc@lysator.liu.se

Supported decryption macs for SSH2	hmac-md5-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-ripemd160-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-md5, hmac-sha1, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
Supported encryption macs for SSH2	hmac-md5-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-ripemd160-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-md5, hmac-sha1, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, gssapi-keyex, gssapi-with-mic, password

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
22	ssh	SSH Remote Login Protocol	ssh	

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 22: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 8 milli seconds

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 977997551 with a standard deviation of 669726561. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(6124 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

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
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 55182	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 5036	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7111	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 5503	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1194	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	14:49:17 GMT
Unreachable (type=3 code=3)	UDP Port 445	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1042	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6771	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable

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	22	0:04:50

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: 437 seconds

Start time: Sun, Dec 25 2022, 14:37:40 GMT

End time: Sun, Dec 25 2022, 14:44:57 GMT

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

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	64.39.111.4	0.12ms	ICMP	
2	64.41.200.245	0.58ms	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:

The ISP network handle is: QUALYS
ISP Network description:
QUALYS, Inc.

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2** ■■□□□
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	12/12/2022

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
Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP	TCP/IP Fingerprint	M4856:7259::22

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 22, the host's uptime is 26 days, 9 hours, and 41 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3** ■■■□□
QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	12/02/2021

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: SSH on TCP port 22.

Vulnerabilities (2)

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): 14:15:43 GMT

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

Information Gathered (24)

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

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.

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

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

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

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	

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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 8 milli seconds
```

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
```

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 880051759 with a standard deviation of 534236556. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(6125 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

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:

TRN-WIN7

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
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 3150	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	14:15:43 GMT
Unreachable (type=3 code=3)	UDP Port 3283	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6912	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6771	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7308	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 21365	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 5000	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1039	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2801	Port Unreachable

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	0:01:10
TCP	445	0:00:59
TCP	49152	0:05:04
TCP	49153	0:05:04
TCP	49154	0:05:04
TCP	49155	0:05:04
TCP	53404	0:05:04
TCP	53405	0:05:04
TCP	65529	0:14:04
UDP	123	0:00:19
UDP	137	0:00:59
UDP	138	0:00:07
UDP	500	0:00:12
UDP	1900	0:00:12

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: 1011 seconds

Start time: Sun, Dec 25 2022, 14:37:23 GMT

End time: Sun, Dec 25 2022, 14:54:14 GMT

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	64.39.111.4	0.26ms	ICMP	
2	64.41.200.247	0.47ms	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:

The ISP network handle is: QUALYS
ISP Network description:
QUALYS, 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
Server

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

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2** ■■□□□
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	12/12/2022

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 456 days, 21 hours, and 23 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

Appendices

Host Comments

64.41.200.245, demo15.s02.sjc01.qualys.com

Please update OpenSSH to the latest versions.Change built-in or default accounts and passwords.

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

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, vulnerabilit es at this level may include full read and write access to files, remote execution of comma ds, 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.