ControlCase
Compliance as a Service

PCI ASV Vulnerability Scan Report (Compliant)

Detailed Report of Findings

ASV Company	ControlCase
Scan Customer Company	Genpact - Global
Title	ASV Scan - Detailed Summary
Scan Date	July 24, 2021
Expiration Date	October 22, 2021
Reference	Genpact_Global_ASV_24_July_2021
IPs Scanned	
38.142.188.30, 69.174.28.138, 59.160.97.246, 202.54.240.182, 125.21.0.182, 125.21.44.66, 182.19.62.165, 122.15.135.129, 216.195.64.30, 216.195.64.34, 4.59.196.78, 67.154.112.26, 50.207.117.50, 12.125.232.106, 122.55.2.142, 222.127.146.122, 32.6.166.114, 32.6.166.118, 121.241.98.81, 125.23.240.158, 115.114.73.26, 32.6.185.174, 32.6.185.182, 32.6.185.186, 12.87.39.214, 157.130.132.82, 12.127.229.197, 12.127.229.198, 97.79.202.49, 97.79.202.50, 97.79.202.51, 97.79.202.52, 97.79.202.53, 97.79.202.54, 121.241.55.129, 15.206.45.65	

Table of Contents

Scope

This document contains the detailed report on the results of the PCI Approved Scanning Vendor (ASV) vulnerability scan and assessment process performed for Genpact - Global PCI ASV. The report presents the vulnerability severity level conventions used in determining the status of compliance with the scan validation requirement of the PCI DSS v2.0/v3.0/v3.1/v3.2.

Vulnerability Level Categorization

Vulnerability Severity Levels

A security vulnerability is a design flaw, which makes a component on your network or the entire 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 severity level of the vulnerability, the successful exploitation of the vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

With a few exceptions, any vulnerability with a CVSS Base Score of 4.0 or higher will result in a non-compliant scan, and all such vulnerabilities must be remediated by the scan customer. To assist in prioritizing the solution or mitigation of identified issues, a severity level has been assigned to each identified vulnerability or misconfiguration. Please refer to the table-1 for guidance.

CVSS Score	Severity Level	Scan Results	Guidance
7.0 through 10.0	High Severity	Fail	To achieve a passing scan, these vulnerabilities must be corrected and the environment must be re-scanned after the corrections (with a report that shows a passing scan).
4.0 through 6.9	Medium Severity	Fail	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical ones (rated 10.0), then those rated 9, followed by those rated 8, 7, etc., until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	Pass	While passing scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

Table 1: Vulnerability Severity Levels

Vulnerability Scoring Reference

IP / Domain	Status
38.142.188.30	Pass
69.174.28.138	Pass
59.160.97.246	Pass
202.54.240.182	Pass
125.21.0.182	Pass
125.21.44.66	Pass
182.19.62.165	Pass
122.15.135.129	Pass
216.195.64.30	Pass
216.195.64.34	Pass
4.59.196.78	Pass
67.154.112.26	Pass
50.207.117.50	Pass
12.125.232.106	Pass
122.55.2.142	Pass
222.127.146.122	Pass
32.6.166.114	Pass
32.6.166.118	Pass
121.241.98.81	Pass
125.23.240.158	Pass
115.114.73.26	Pass
32.6.185.174	Pass
32.6.185.182	Pass
32.6.185.186	Pass
12.87.39.214	Pass
157.130.132.82	Pass
12.127.229.197	Pass
12.127.229.198	Pass
97.79.202.49	Pass
97.79.202.50	Pass
97.79.202.51	Pass
97.79.202.52	Pass
97.79.202.53	Pass
97.79.202.54	Pass
121.241.55.129	Pass
15.206.45.65	Pass

Detailed Vulnerability Results

This section gives the details on the scan results sorted by IP address and vulnerability severity.

No	Vulnerability Name &Finding	Severity Level / Compliance Status	Affected IP Addresses/ Domain	Threat	Impact	Solution	CVE ID	CVSS V2 Score	Category
1	Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode Findings: isakmp hash(key + identity): 206bc1d475071adae796 e0551d089efe7843019b.	Low / Pass	38.142.188.30 : 500 / udp	IKE is used during Phase 1 and Phase 2 of establishing an IPSec connection. Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used. QID Detection Logic This QID checks if the peer accepts the proposal which specifies 'Pre-shared key' as authentication method in aggressive mode,enabled with pre-shared keys during IKE phase 1 negotiation and returns the hash of ISAKMP response.	Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. For more information about this type of attack, visit http://www.ernw.de/download/pskattack.pdf (http://www.ernw.de/download/pskattack.pdf) .	IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.	CVE-2002-1623	5.0	General remote services
2	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 22:52:01 GMT.	Low / Pass	38.142.188.30	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.				0	TCP/IP

3	Host Name Not Available Findings: .	Low / Pass	38.142.188.30	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
4	DNS Host Name Findings: IP address Host name 38.142.188.30 No registered hostname.	Low / Pass	38.142.188.30	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
5	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.50ms ICMP 2 216.35.14.45 0.38ms ICMP 3 *.*.*.* 0.00ms Other 21 4 67.14.43.82 3.70ms ICMP 5 67.14.34.38 4.41ms ICMP 6 4.68.62.77 4.93ms ICMP 7 *.*.*.* 0.00ms Other 21 8 154.54.43.9 7.09ms ICMP 9 154.54.44.138 31.69ms ICMP 10 154.54.41.146 31.72ms ICMP 11 154.54.5.90 137.96ms ICMP 12 154.54.42.166 53.62ms ICMP 13 154.54.81.102 53.43ms ICMP 14 154.24.11.142 53.58ms ICMP 15 38.142.188.30 52.93ms ICMP.	Low / Pass	38.142.188.30	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.				0	Information gathering
6	Target Network Information Findings: The network handle is: COGENT-A Network description: PSINet, Inc..	Low / Pass	38.142.188.30	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.	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering
7	Internet Service Provider Findings: The ISP network handle is: LVLT-ORG-4-8 ISP Network description: Level 3 Parent, LLC.	Low / Pass	38.142.188.30	The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target	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.			0	Information gathering

				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.					
8	Host Scan Time Findings: Scan duration: 690 seconds Start time: Fri, Jul 23 2021, 21:14:13 GMT End time: Fri, Jul 23 2021, 21:25:43 GMT.	Low / Pass	38.142.188.30	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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.				0	Information gathering
9	Scan Activity per Port Findings: Protocol Port Time UDP 123 0:01:24 UDP 161 0:02:27 UDP 500 0:02:48.	Low / Pass	38.142.188.30	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				0	Information gathering

				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.					
10	Remote Access or Management Service Detected Findings: Service name: SNMP on UDP port 161. Service name: ISAKMP on UDP port 500..	Low / Pass	38.142.188.30	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.	Consequences vary by the type of attack.	Expose the remote access or remote management services only to the system administrators or intended users of the system.		0	General remote services
11	Open UDP Services List Findings: Port IANA Assigned Ports/Services Description Service Detected 123 ntp Network Time Protocol ntp 161 snmp SNMP snmp 500 isakmp isakmp isakmp.	Low / Pass	38.142.188.30	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.	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	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) .		0	TCP/IP
12	Firewall Detected Findings: Some of the ports filtered by the firewall are: 22, 23, 6000.	Low / Pass	38.142.188.30	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control				0	Firewall

	Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 22-23,545-617,4501-5491,5493-5504,5506-5549,5551-5559,5561-5569,5571-5579, 5581-5630,5632-6013, 6015-6128,6130-7006, 7008-7009,7011-7572.			lists (ACLs).					
13	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 22:52:01 GMT.	Low / Pass	38.142.188.30	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.	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).	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.	CVE-1999-0524	0	TCP/IP
14	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo	Low / Pass	59.160.97.246	ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is				0	TCP/IP

	Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 19:09:14 GMT.			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.					
15	DNS Host Name Findings: IP address Host name 59.160.97.246 59.160.97.246.static.vsnl.net.in.	Low / Pass	59.160.97.246	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
16	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.29ms ICMP 2 216.35.14.45 0.79ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 3.83ms ICMP 5 67.14.34.38 9.59ms ICMP 6 4.68.62.77 7.72ms ICMP 7 4.69.209.149 5.73ms ICMP 8 4.68.63.214 5.47ms ICMP 9 63.243.205.1 15.09ms ICMP 10 63.243.205.73 14.72ms ICMP 11 63.243.251.1 14.83ms ICMP 12 63.243.250.59 14.48ms ICMP 13 66.110.59.122 241.79ms ICMP 14 *.*.*.* 0.00ms Other 80 15 59.160.97.246 273.25ms ICMP.	Low / Pass	59.160.97.246	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.				0	Information gathering
17	Target Network Information Findings: The network handle is: APNIC-59 Network description: Asia Pacific Network Information Centre.	Low / Pass	59.160.97.246	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 can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering

				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.					
18	Internet Service Provider Findings: The ISP network handle is: NET-66-110-59-0-1 ISP Network description: Tata Communications,Ltd. LOSANGELES-LVW-TATAC.	Low / Pass	59.160.97.246	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.	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.			0	Information gathering
19	Host Names Found Findings: Host Name Source 59.160.97.246.static .vsnl.net.in FQDN.	Low / Pass	59.160.97.246	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
20	Host Scan Time Findings: Scan duration: 2490 seconds Start time: Fri, Jul 23 2021, 19:09:03 GMT End time: Fri, Jul 23 2021, 19:50:33 GMT.	Low / Pass	59.160.97.246	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.				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
21	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535.	Low / Pass	59.160.97.246	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
22	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 19:09:14 GMT.	Low / Pass	59.160.97.246	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.	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).	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	CVE-1999-0524	0	TCP/IP

						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.			
23	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 22:43:16 GMT.	Low / Pass	202.54.240.182	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.				0	TCP/IP
24	DNS Host Name Findings: IP address Host name 202.54.240.182 delhi -202.54.240.182.vsnl .net.in.	Low / Pass	202.54.240.182	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
25	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.52ms ICMP 2 216.35.14.45 0.38m s ICMP 3 *.*.*.* 0.00ms Oth er 21 4 67.14.43.82 3.71ms	Low / Pass	202.54.240.182	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.				0	Information gathering

	ICMP 5 67.14.34.38 18.46ms ICMP 6 4.68.62.77 5.12ms ICMP 7 *.*.*.* 0.00ms Other 21 8 4.68.63.214 6.06ms ICMP 9 63.243.205.1 15.18ms ICMP 10 63.243.205.73 14.59ms ICMP 11 63.243.251.1 18.98ms ICMP 12 63.243.250.59 14.64ms ICMP 13 66.110.59.122 241.58ms ICMP 14 *.*.*.* 0.00ms Other 21 15 202.54.240.182 270.58ms ICMP.								
26	Target Network Information Findings: The network handle is: TATACOMM-IN Network description: Internet Service Provider.	Low / Pass	202.54.240.182	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.	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering
27	Internet Service Provider Findings: The ISP network handle is: NET-66-110-59-0-1 ISP Network description: Tata Communications,Ltd. LOSANGELES-LVW-TATAC.	Low / Pass	202.54.240.182	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.	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.			0	Information gathering
28	Host Names Found Findings: Host Name Source delhi-202.54.240.182.vsnl.net.in FQDN.	Low / Pass	202.54.240.182	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
29	Host Scan Time	Low / Pass	202.54.240.182	The Host Scan Time				0	Information gathering

	Findings: Scan duration: 1474 seconds Start time: Fri, Jul 23 2021, 22:43:18 GMT End time: Fri, Jul 23 2021, 23:07:52 GMT.			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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
30	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 22:43:16 GMT.	Low / Pass	202.54.240.182	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.	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).	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	CVE-1999-0524	0	TCP/IP

						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.			
31	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Unreachable (type=3 code=13) (Various) C ommunication Prohibited.	Low / Pass	125.21.0.182	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.				0	TCP/IP
32	Host Name Not Available Findings: .	Low / Pass	125.21.0.182	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
33	DNS Host Name Findings: IP address Host name 125.21.0.182 No registered hostname.	Low / Pass	125.21.0.182	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering

34	Host Scan Time Findings: Scan duration: 2495 seconds Start time: Fri, Jul 23 2021, 21:14:24 GMT End time: Fri, Jul 23 2021, 21:55:59 GMT.	Low / Pass	125.21.0.182	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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.				0	Information gathering
35	Firewall Detected Findings: Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-178,180-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100, 2102-2146,2148-2512, 2514-2701,2703-3388, 3390-5491,5493-5504, 5506-5549, 5551-5559,5561-5569, 5571-5579,5581-5630, 5632-6013,6015-6128, 6130-7006, 7008-7009,7011-9098, 9100-9989,9991-10109 ,10111-42423,42425-65535.	Low / Pass	125.21.0.182	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
36	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Unreachable (type=3	Low / Pass	125.21.44.66	ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is				0	TCP/IP

	code=13) (Various) Communication Prohibited.			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.					
37	Host Name Not Available Findings: .	Low / Pass	125.21.44.66	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
38	DNS Host Name Findings: IP address Host name 125.21.44.66 No registered hostname.	Low / Pass	125.21.44.66	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
39	Host Scan Time Findings: Scan duration: 2500 seconds Start time: Fri, Jul 23 2021, 23:40:35 GMT End time: Sat, Jul 24 2021, 00:22:15 GMT.	Low / Pass	125.21.44.66	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.				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
40	Firewall Detected Findings: Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-178,180-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100, 2102-2146,2148-2512, 2514-2701,2703-3388, 3390-5491,5493-5504, 5506-5549, 5551-5559,5561-5569, 5571-5579,5581-5630, 5632-6013,6015-6128, 6130-7006, 7008-7009,7011-9098, 9100-9989,9991-10109,10111-42423,42425-65535.	Low / Pass	125.21.44.66	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
41	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Unreachable (type=3 code=13) (Various) Communication Prohibited.	Low / Pass	216.195.64.30	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.				0	TCP/IP
42	DNS Host Name Findings: IP address Host name 216.195.64.30 216-19	Low / Pass	216.195.64.30	The fully qualified domain name of this host, if it was				0	Information gathering

	5-64-30.cncndc.net.			obtained from a DNS server, is displayed in the RESULT section.					
43	Host Names Found Findings: Host Name Source 216-195-64-30.cncndc .net FQDN.	Low / Pass	216.195.64.30	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
44	Host Scan Time Findings: Scan duration: 2506 seconds Start time: Fri, Jul 23 2021, 19:50:33 GMT End time: Fri, Jul 23 2021, 20:32:19 GMT.	Low / Pass	216.195.64.30	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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.				0	Information gathering
45	Firewall Detected Findings: Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035, 2037-2100, 2102-2146,2148-2512, 2514-2701,2703-3388, 3390-5491,5493-5504, 5506-5549, 5551-5559,5561-5569, 5571-5579,5581-5630,	Low / Pass	216.195.64.30	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall

	5632-6013,6015-6128,6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535.								
46	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 12:28:43 GMT.	Low / Pass	4.59.196.78	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.				0	TCP/IP
47	DNS Host Name Findings: IP address Host name 4.59.196.78 one-source.ear1.dallas1.level3.net.	Low / Pass	4.59.196.78	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
48	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.45ms ICMP 2 216.35.14.45 2.00ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 3.84ms ICMP 5 67.14.34.38 10.37ms ICMP 6 4.68.62.77 4.93ms ICMP 7 *.*.*.* 0.00ms Other 80 8 4.59.196.78 139.97ms ICMP.	Low / Pass	4.59.196.78	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.				0	Information gathering
49	Target Network Information Findings: The network handle is: LVLT-ORG-4-8 Network description: Level 3 Parent, LLC.	Low / Pass	4.59.196.78	The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering

				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.					
50	Internet Service Provider Findings: The ISP network handle is: CENTURYLINK-LEGACY-PICNIC-SPACE ISP Network description: CenturyLink Communications, LLC.	Low / Pass	4.59.196.78	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.	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.			0	Information gathering
51	Host Names Found Findings: Host Name Source one-source.ear1.dallas1.level3.net FQDN.	Low / Pass	4.59.196.78	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
52	Host Scan Time Findings: Scan duration: 2492 seconds Start time: Fri, Jul 23 2021, 19:09:03 GMT End time: Fri, Jul 23 2021, 19:50:35 GMT.	Low / Pass	4.59.196.78	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				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
53	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-178,180-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100, 2102-2146,2148-2512, 2514-2701,2703-3388, 3390-5491,5493-5504, 5506-5549, 5551-5559,5561-5569, 5571-5579,5581-5630, 5632-6013,6015-6128, 6130-7006, 7008-7009,7011-9098, 9100-9989,9991-10109,10111-42423,42425-65535.	Low / Pass	4.59.196.78	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
54	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 12:28:43 GMT.	Low / Pass	4.59.196.78	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.	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).	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	CVE-1999-0524	0	TCP/IP

						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.			
55	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply.	Low / Pass	50.207.117.50	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.				0	TCP/IP
56	IP ID Values Randomness Findings: IP ID changes observed (network order) for port 179: 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: 33 milli seconds.	Low / Pass	50.207.117.50	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				0	TCP/IP

				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.					
57	Host Uptime Based on TCP TimeStamp Option Findings: Based on TCP timestamps obtained via port 179, the host's uptime is 214 days, 16 hours, and 55 minutes. The TCP timestamps from the host are in units of 10 milliseconds..	Low / Pass	50.207.117.50	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.				0	TCP/IP
58	Degree of Randomness of TCP Initial Sequence Numbers Findings: Average change between subsequent TCP initial sequence numbers is 1026841806 with a standard deviation of 560206637. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5038 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard..	Low / Pass	50.207.117.50	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.				0	TCP/IP
59	DNS Host Name Findings: IP address Host name 50.207.117.50 50-207 -117-50-static.hfc.c omcastbusiness.net.	Low / Pass	50.207.117.50	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
60	Traceroute	Low / Pass	50.207.117.50	Traceroute describes the path in realtime				0	Information gathering

	Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.36ms ICMP 2 216.35.14.45 0.43ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 3.78ms ICMP 5 67.14.34.38 4.34ms ICMP 6 4.68.62.77 5.01ms ICMP 7 4.68.39.114 6.17ms ICMP 8 96.110.32.245 5.70 ms ICMP 9 68.86.166.130 5.51 ms ICMP 10 96.110.38.89 12.38ms ICMP 11 96.110.45.161 12.29ms ICMP 12 96.110.45.242 33.59ms ICMP 13 96.108.67.234 33.11ms ICMP 14 162.151.187.50 33.15ms ICMP 15 50.207.117.50 32.94ms ICMP.			from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.					
61	Target Network Information Findings: The network handle is: CCCH3-4 Network description: Comcast Cable Communications, LLC.	Low / Pass	50.207.117.50	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.	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering
62	Internet Service Provider Findings: The ISP network handle is: NET-68-86-128-0-1 ISP Network description: Comcast Cable Communications, Inc. COMCAST-8.	Low / Pass	50.207.117.50	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.	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.			0	Information gathering
63	Host Names Found Findings: Host Name Source 50-207-117-50-static	Low / Pass	50.207.117.50	The following host names were discovered for this computer using				0	Information gathering

	.hfc.comcastbusiness .net FQDN.			various methods such as DNS look up, NetBIOS query, and SQL server name query.					
64	Host Scan Time Findings: Scan duration: 2360 seconds Start time: Fri, Jul 23 2021, 23:19:46 GMT End time: Fri, Jul 23 2021, 23:59:06 GMT.	Low / Pass	50.207.117.50	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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.				0	Information gathering
65	Scan Activity per Port Findings: Protocol Port Time TCP 179 0:00:56 TCP 541 0:04:40.	Low / Pass	50.207.117.50	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.				0	Information gathering

66	Open TCP Services List Findings: Port IANA Assigned Ports/Services Description Service Detected OS On Redirected Port 179 bgp Border Gateway Protocol unknown 541 uucp-rlogin uucp-rlogin unknown.	Low / Pass	50.207.117.50	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).	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	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) .		0	TCP/IP
67	Operating System Detected Findings: Operating System Technique ID Linux 2.6 TCP/IP Fingerprint U6388:179.	Low / Pass	50.207.117.50	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	Not applicable.	Not applicable.		0	Information gathering

				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.					
68	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-112,114-178,180-540,542-6128,6130-65535.	Low / Pass	50.207.117.50	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
69	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp	Low / Pass	12.125.232.106	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				0	TCP/IP

	Request 20:17:08 GMT.			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.					
70	Host Name Not Available Findings: .	Low / Pass	12.125.232.106	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
71	DNS Host Name Findings: IP address Host name 12.125.232.106 No registered hostname.	Low / Pass	12.125.232.106	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
72	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.61ms ICMP 2 216.35.14.45 0.58ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 24.29ms ICMP 5 67.14.34.38 4.51ms ICMP 6 4.68.62.77 5.17ms ICMP 7 *.*.*.* 0.00ms Other 80 8 192.205.32.209 8.61ms ICMP 9 12.122.114.6 58.32ms ICMP 10 12.122.1.173 57.06ms ICMP 11 12.122.152.137 55.99ms ICMP 12 12.122.152.209 54.81ms ICMP 13 12.125.232.106 55.71ms ICMP.	Low / Pass	12.125.232.106	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.				0	Information gathering
73	Target Network Information Findings: The network handle is: NET-12-125-0-0-1 Network description: AT&T Worldnet Services ATTSVI-12-125-0-0-1.	Low / Pass	12.125.232.106	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	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering

				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.					
74	Internet Service Provider Findings: The ISP network handle is: NET-12-122-0-0-1 ISP Network description: AT&T Worldnet Services ATTSVI-12-122-0-0.	Low / Pass	12.125.232.106	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.	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.			0	Information gathering
75	Host Scan Time Findings: Scan duration: 2473 seconds Start time: Fri, Jul 23 2021, 20:16:58 GMT End time: Fri, Jul 23 2021, 20:58:11 GMT.	Low / Pass	12.125.232.106	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.				0	Information gathering

				For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
76	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535.	Low / Pass	12.125.232.106	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
77	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 20:17:08 GMT.	Low / Pass	12.125.232.106	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.	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).	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	CVE-1999-0524	0	TCP/IP

						TCP/IP stacks. It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.			
78	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 22:27:05 GMT.	Low / Pass	122.55.2.142	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.				0	TCP/IP
79	DNS Host Name Findings: IP address Host name 122.55.2.142 122.55.2.142.pldt.net.	Low / Pass	122.55.2.142	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
80	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.41ms ICMP 2 216.35.14.45 0.36ms ICMP 3 *.*.*.* 0.00ms Other 21 4 67.14.43.82 3.72ms ICMP 5 67.14.34.38 4.39ms ICMP 6 4.68.62.77 5.00ms ICMP 7 4.69.153.129 11.83ms ICMP 8 4.26.2.6 12.13ms ICMP 9 210.213.133.205 154.97ms ICMP	Low / Pass	122.55.2.142	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.				0	Information gathering

	10 210.213.133.165 1 59.55ms ICMP 11 210.213.133.0 159 .43ms ICMP 12 122.55.2.142 160. 62ms ICMP.								
81	Internet Service Provider Findings: The ISP network handle is: IPG ISP Network description: IPG.	Low / Pass	122.55.2.142	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.	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.			0	Information gathering
82	Cisco IOS Installed on Target Host Findings: Cisco IOS 11-15.	Low / Pass	122.55.2.142	Cisco IOS installation was found on target host.				0	Information gathering
83	Host Names Found Findings: Host Name Source 122.55.2.142.pldt.ne t FQDN.	Low / Pass	122.55.2.142	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
84	Host Scan Time Findings: Scan duration: 975 seconds Start time: Fri, Jul 23 2021, 22:27:03 GMT End time: Fri, Jul 23 2021, 22:43:18 GMT.	Low / Pass	122.55.2.142	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				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
85	Scan Activity per Port Findings: Protocol Port Time TCP 53 0:01:16 UDP 53 0:05:05 UDP 123 0:01:24 UDP 161 0:02:27.	Low / Pass	122.55.2.142	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.				0	Information gathering
86	Remote Access or Management Service Detected Findings: Service name: SNMP on UDP port 161..	Low / Pass	122.55.2.142	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.	Consequences vary by the type of attack.	Expose the remote access or remote management services only to the system administrators or intended users of the system.		0	General remote services
87	Open TCP Services List Findings: Port IANA Assigned Ports/Services Descr iption Service Detected OS On Redirected Port 53 domain Domain Name Server DNS	Low / Pass	122.55.2.142	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	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	Shut down any unknown or unused service on the list. If you have difficulty figuring out		0	TCP/IP

	Server.			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).		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) .			
88	Open UDP Services List Findings: Port IANA Assigned Ports/Services Description Service Detected 53 domain Domain Name Server named udp 123 ntp Network Time Protocol ntp 161 snmp SNMP snmp.	Low / Pass	122.55.2.142	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.	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	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) .		0	TCP/IP
89	Operating System Detected Findings: Operating System Technique ID Cisco IOS 11-15 TCP/IP Fingerprint U1053:53.	Low / Pass	122.55.2.142	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	Not applicable.	Not applicable.		0	Information gathering

				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.					

90	Named Daemon Version Number Disclosure Vulnerability Findings: unbound 1.4.22.	Low / Pass	122.55.2.142 : 53 / tcp	Named is the daemon used to provide the DNS translation service.	If successfully exploited, unauthorized users can determine which version of 'named' is running on this host. This is very dangerous since it enables aggressive intruders to prepare a specific attack for the version being used.	Unless it is required on this host, disable this feature.		0	DNS and BIND
91	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 22:27:05 GMT.	Low / Pass	122.55.2.142	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.	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).	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.	CVE-1999-0524	0	TCP/IP
92	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo	Low / Pass	222.127.146.122	ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is				0	TCP/IP

	Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request - Unreachable (type=3 code=13) (Various) Communication Prohibited.			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.					
93	Host Name Not Available Findings: .	Low / Pass	222.127.146.122	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
94	DNS Host Name Findings: IP address Host name 222.127.146.122 No registered hostname.	Low / Pass	222.127.146.122	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
95	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.39ms ICMP 2 216.35.14.45 1.11ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 5.07ms ICMP 5 67.14.34.38 4.34ms ICMP 6 4.68.62.77 5.04ms ICMP 7 4.69.137.201 21.96ms ICMP 8 4.59.234.38 21.83ms ICMP 9 120.28.0.85 148.13ms ICMP 10 *.*.*.* 0.00ms Other 80 11 222.127.146.122 158.23ms ICMP.	Low / Pass	222.127.146.122	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.				0	Information gathering
96	Internet Service Provider Findings: The ISP network handle is: LVLT-ORG-4-8 ISP Network description: Level 3 Parent, LLC.	Low / Pass	222.127.146.122	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	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.			0	Information gathering

				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.					
97	Host Scan Time Findings: Scan duration: 2497 seconds Start time: Fri, Jul 23 2021, 21:13:52 GMT End time: Fri, Jul 23 2021, 21:55:29 GMT.	Low / Pass	222.127.146.122	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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.				0	Information gathering
98	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,	Low / Pass	222.127.146.122	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall

	2037-2100, 2102-2146,2148-2512, 2514-2701,2703-3388, 3390-5491,5493-5504, 5506-5549, 5551-5559,5561-5569, 5571-5579,5581-5630, 5632-6013,6015-6128, 6130-7006, 7008-7009,7011-9098, 9100-9989,9991-10109 ,10111-42423,42425-65535.								
99	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 21:55:33 GMT.	Low / Pass	115.114.73.26	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.				0	TCP/IP
100	DNS Host Name Findings: IP address Host name 115.114.73.26 115.114.73.26.static-delhi.vsnl.net.in.	Low / Pass	115.114.73.26	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
101	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.35ms ICMP 2 216.35.14.45 0.34ms ICMP 3 *.*.*.* 0.00ms Other 21 4 67.14.43.82 3.76ms ICMP 5 67.14.34.38 4.44ms ICMP 6 4.68.62.77 5.00ms ICMP 7 4.69.209.153 5.78ms ICMP 8 4.68.63.214 5.48ms ICMP 9 63.243.205.1 15.02ms ICMP 10 209.58.86.36 14.86ms ICMP 11 63.243.251.1 14.73ms ICMP 12 63.243.250.59 14.	Low / Pass	115.114.73.26	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.				0	Information gathering

	65ms ICMP 13 66.110.59.114 240.64ms ICMP 14 *.*.*.* 0.00ms Other 21 15 115.114.73.26 277.33ms ICMP.								
102	Internet Service Provider Findings: The ISP network handle is: NET-66-110-59-0-1 ISP Network description: Tata Communications,Ltd. LOSANGELES-LVW-TATAC.	Low / Pass	115.114.73.26	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.	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.			0	Information gathering
103	Host Names Found Findings: Host Name Source 115.114.73.26.static-delhi.vsnl.net.in FQDN.	Low / Pass	115.114.73.26	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
104	Host Scan Time Findings: Scan duration: 1578 seconds Start time: Fri, Jul 23 2021, 21:55:29 GMT End time: Fri, Jul 23 2021, 22:21:47 GMT.	Low / Pass	115.114.73.26	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				0	Information gathering

				perform parallel host scanning on all scanners. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
105	Scan Activity per Port Findings: Protocol Port Time UDP 161 0:02:27.	Low / Pass	115.114.73.26	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.				0	Information gathering
106	Remote Access or Management Service Detected Findings: Service name: SNMP on UDP port 161..	Low / Pass	115.114.73.26	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.	Consequences vary by the type of attack.	Expose the remote access or remote management services only to the system administrators or intended users of the system.		0	General remote services
107	Open UDP Services List Findings: Port IANA Assigned Ports/Services Descr iption Service Detected 161 snmp SNMP snmp.	Low / Pass	115.114.73.26	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	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	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		0	TCP/IP

				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.		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) .			
108	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 21:55:33 GMT.	Low / Pass	115.114.73.26	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.	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).	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.	CVE-1999-0524	0	TCP/IP

109	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Unreachable (type=3 code=3) UDP Port 1038 Port Unreachable Time Stamp (type=14 code=0) Time Stamp Request 21:25:16 GMT Unreachable (type=3 code=3) UDP Port 7778 Port Unreachable Unreachable (type=3 code=3) UDP Port 17185 Port Unreachable Unreachable (type=3 code=3) UDP Port 4781 Port Unreachable Unreachable (type=3 code=3) UDP Port 98 Port Unreachable Unreachable (type=3 code=3) UDP Port 7301 Port Unreachable Unreachable (type=3 code=3) UDP Port 1600 Port Unreachable Unreachable (type=3 code=3) UDP Port 51100 Port Unreachable Unreachable (type=3 code=3) UDP Port 517 Port Unreachable Unreachable (type=3 code=3) UDP Port 31785 Port Unreachable Unreachable (type=3 code=2) IP with High Protocol Protocol Unreachable.	Low / Pass	12.87.39.214	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.				0	TCP/IP
110	Host Name Not Available Findings: .	Low / Pass	12.87.39.214	Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.				0	TCP/IP
111	DNS Host Name Findings: IP address Host name 12.87.39.214 No registered hostname.	Low / Pass	12.87.39.214	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
112	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.40ms ICMP 2 216.35.14.45 0.44ms ICMP 3 *.*.*.* 0.00ms Other 21 4 67.14.43.82 3.74ms ICMP 5 67.14.34.38 4.58ms ICMP 6 4.68.62.77 5.20ms ICMP 7 *.*.*.* 0.00ms Other 21 8 192.205.32.209 7.51ms ICMP	Low / Pass	12.87.39.214	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.				0	Information gathering

	9 12.122.149.134 128 .67ms ICMP 10 12.122.28.121 132 .01ms ICMP 11 12.122.2.81 142.2 2ms ICMP 12 12.123.235.93 142 .12ms ICMP 13 12.87.39.214 143. 75ms TCP 21.								
113	Target Network Information Findings: The network handle is: NET-12-86-0-0-1 Network description: AT&T Worldnet Services ATTSVC-12-86-0-0.	Low / Pass	12.87.39.214	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.	This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.			0	Information gathering
114	Internet Service Provider Findings: The ISP network handle is: NET-12-122-0-0-1 ISP Network description: AT&T Worldnet Services ATTSVI-12-122-0-0.	Low / Pass	12.87.39.214	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.	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.			0	Information gathering
115	Host Scan Time Findings: Scan duration: 1076 seconds Start time: Fri, Jul 23 2021, 21:25:16 GMT End time: Fri, Jul 23 2021, 21:43:12 GMT.	Low / Pass	12.87.39.214	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.				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
116	Scan Activity per Port Findings: Protocol Port Time UDP 19 0:00:07 UDP 37 0:00:07 UDP 68 0:00:07 UDP 123 0:00:19 UDP 161 0:00:56 UDP 514 0:00:07 UDP 1900 0:00:12.	Low / Pass	12.87.39.214	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.				0	Information gathering
117	Open UDP Services List Findings: Port IANA Assigned Ports/Services Description Service Detected 19 chargen Character Generator unknown 37 time Time unknown 68 bootpc Bootstrap Protocol Client unknown 123 ntp Network Time Protocol unknown 161 snmp SNMP unknown 514 syslog syslog unknown 1900 unknown unknown unknown.	Low / Pass	12.87.39.214	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	Unauthorized users can exploit this information to test vulnerabilities in each of the open services.	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,		0	TCP/IP

				filter/block/drop UDP packets for only a few ports. Both cases are uncommon.		visit the CERT Web site (http://www. cert.org) .			
118	Firewall Detected Findings: Some of the ports filtered by the firewall are: 22. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 22,49,123,514,830.	Low / Pass	12.87.39.214	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
119	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 21:25:16 GMT.	Low / Pass	12.87.39.214	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.	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).	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.	CVE-1999-0524	0	TCP/IP

120	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 22:49:11 GMT.	Low / Pass	97.79.202.49	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.				0	TCP/IP
121	DNS Host Name Findings: IP address Host name 97.79.202.49 rrcs-97-79-202-49.sw.biz.rr.com.	Low / Pass	97.79.202.49	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
122	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.33ms ICMP 2 216.35.14.45 0.36ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 3.87ms ICMP 5 67.14.34.38 11.01ms ICMP 6 4.68.62.77 5.14ms ICMP 7 *.*.*.* 0.00ms Other 80 8 4.68.74.178 7.00ms ICMP 9 66.109.6.8 144.93ms UDP 80 10 66.109.6.7 142.07ms ICMP 11 107.14.19.36 125.88ms ICMP 12 66.109.6.1 131.22ms ICMP 13 66.109.6.53 142.51ms ICMP 14 24.175.49.1 132.69ms ICMP 15 24.175.49.9 155.80ms ICMP 16 24.175.49.254 144.31ms ICMP 17 97.77.0.83 141.15ms ICMP 18 97.77.0.80 134.68ms ICMP 19 97.77.1.236 147.34ms ICMP 20 67.79.253.71 153.	Low / Pass	97.79.202.49	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.				0	Information gathering

	42ms ICMP 21 97.79.202.49 154. 04ms ICMP.								
123	Internet Service Provider Findings: The ISP network handle is: RR-COMM ISP Network description: Charter Communications Inc.	Low / Pass	97.79.202.49	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.	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.			0	Information gathering
124	Host Names Found Findings: Host Name Source rrcs-97-79-202-49.sw .biz.rr.com FQDN.	Low / Pass	97.79.202.49	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
125	Host Scan Time Findings: Scan duration: 1845 seconds Start time: Fri, Jul 23 2021, 22:49:01 GMT End time: Fri, Jul 23 2021, 23:19:46 GMT.	Low / Pass	97.79.202.49	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.				0	Information gathering

				For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
126	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,2514-2701,2703-2868,2870-3388,3390-5491,5493-5504,5506-5549,5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-33433,33453-33454,33497,33535-42423,42425-65535.	Low / Pass	97.79.202.49	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
127	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 22:49:11 GMT.	Low / Pass	97.79.202.49	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.	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).	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	CVE-1999-0524	0	TCP/IP

						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.			
128	ICMP Replies Received Findings: ICMP Reply Type Triggered By Additional Information Echo (type=0 code=0) Echo Request Echo Reply Time Stamp (type=14 code=0) Time Stamp Request 20:32:54 GMT.	Low / Pass	121.241.55.129	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.				0	TCP/IP
129	DNS Host Name Findings: IP address Host name 121.241.55.129 121.241.55.129.static-hyderabad.vsnl.net.in.	Low / Pass	121.241.55.129	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.				0	Information gathering
130	Traceroute Findings: Hops IP Round Trip Time Probe Port 1 64.39.111.3 0.29ms ICMP 2 216.35.14.45 0.35ms ICMP 3 *.*.*.* 0.00ms Other 80 4 67.14.43.82 3.72ms ICMP 5 67.14.34.38 4.40ms ICMP 6 4.68.62.77 5.10ms ICMP 7 4.69.209.149 5.73ms ICMP 8 4.68.63.214 5.51ms	Low / Pass	121.241.55.129	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.				0	Information gathering

	ICMP 9 63.243.205.1 255.9 3ms ICMP 10 63.243.128.28 261 .39ms ICMP 11 80.231.131.72 251 .82ms ICMP 12 216.6.90.22 258.4 3ms UDP 80 13 180.87.39.22 251. 58ms ICMP 14 180.87.39.26 253. 46ms ICMP 15 180.87.39.22 256. 24ms ICMP 16 121.241.55.129 26 7.34ms ICMP.								
131	Internet Service Provider Findings: The ISP network handle is: APNIC-180 ISP Network description: Asia Pacific Network Information Centre.	Low / Pass	121.241.55.129	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.	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.			0	Information gathering
132	Host Names Found Findings: Host Name Source 121.241.55.129.stati c-hyderabad.vsnl.net .in FQDN.	Low / Pass	121.241.55.129	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
133	Host Scan Time Findings: Scan duration: 2500 seconds Start time: Fri, Jul 23 2021, 20:32:44 GMT End time: Fri, Jul 23 2021, 21:14:24 GMT.	Low / Pass	121.241.55.129	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				0	Information gathering

				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. For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
134	Firewall Detected Findings: Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443. Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535.	Low / Pass	121.241.55.129	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall
135	ICMP Timestamp Request Findings: Timestamp of host (network byte ordering): 20:32:54 GMT.	Low / Pass	121.241.55.129	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.	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).	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	CVE-1999-0524	0	TCP/IP

						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.			
136	Host Names Found Findings: Host Name Source ec2-15-206-45-65.ap-south-1.compute.amazonaws.com FQDN.	Low / Pass	15.206.45.65	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.				0	Information gathering
137	Host Scan Time Findings: Scan duration: 1572 seconds Start time: Fri, Jul 23 2021, 19:09:03 GMT End time: Fri, Jul 23 2021, 19:35:15 GMT.	Low / Pass	15.206.45.65	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. For host running the Qualys Windows agent				0	Information gathering

				this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.					
138	Firewall Detected Findings: Listed below are the ports filtered by the firewall. No response has been received when any of these ports are probed. 1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100, 2102-2146,2148-2512, 2514-2701,2703-2868, 2870-3388,3390-5491, 5493-5504, 5506-5549,5551-5559, 5561-5569,5571-5579, 5581-5630,5632-6013, 6015-6128, 6130-7006,7008-7009, 7011-9098,9100-9989, 9991-10109,10111-42423,42425-65535.	Low / Pass	15.206.45.65	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).				0	Firewall