Qualys. Enterprise TruRisk™ Platform

Scan Results

April 07, 2025

This report was generated with an evaluation version of Qualys

Report Summary	
User Name:	Blip Blop
Login Name:	hmeab8bb
Company:	Homelab
User Role:	Manager
Address:	Turo
Zip:	201306
Country:	India
Created:	04/07/2025 at 09:42:43 PM (GMT+0530)
Launch Date:	04/06/2025 at 08:57:58 PM (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1743953278.20729
External Scanners:	103.75.173.15 (Scanner 14.6.12-1, Vulnerability Signatures 2.6.291-4)
Duration:	00:15:35
Title:	ngork
Asset Groups:	-
IPs:	
Excluded IPs:	-
FQDNs:	3946-122-161-74-80.ngrok-free.app
Options Profile:	Qualys Recommended Option Profile

Summary of Vulnerabilities

Vulnerabilities Total	27

Security Risk (Avg)	1.0

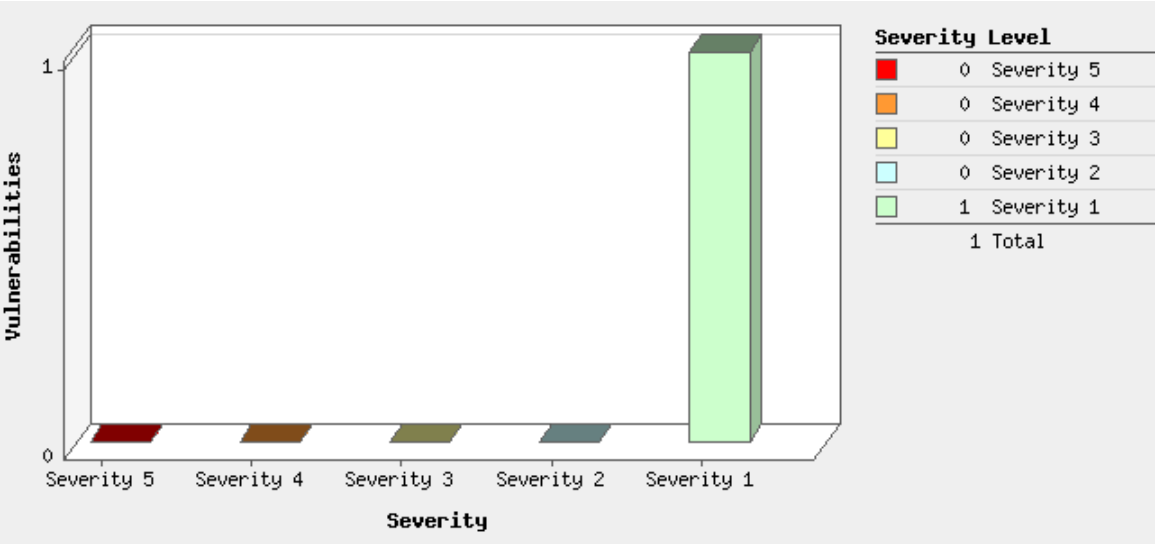
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	2	2
2	0	0	1	1
1	1	0	23	24
Total	1	0	26	27

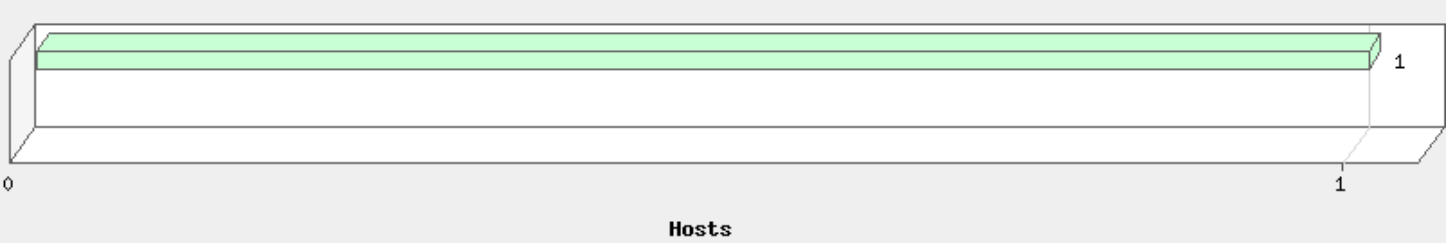
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	8	8
General remote services	0	0	7	7
TCP/IP	1	0	5	6
Web server	0	0	5	5
Firewall	0	0	1	1
Total	1	0	26	27

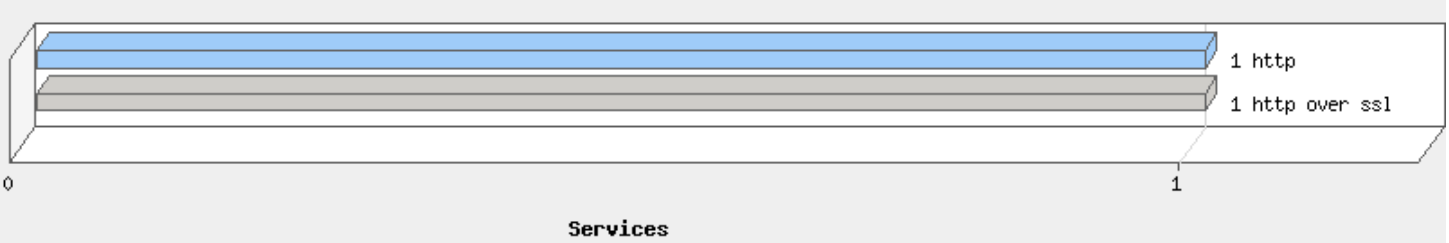
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

3.6.98.232 (3946-122-161-74-80.ngrok-free.app, -)

Vulnerabilities (1)

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	2.1
Category:	TCP/IP	CVSS Temporal:	1.8
Associated CVEs:	CVE-1999-0524		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	11/26/2024	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		

PCI Vuln: No

THREAT:

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

ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only be Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.

Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:

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

SOLUTION:

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

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

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-1999-0524
Description:	threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit exploit repository
Link:	https://github.com/threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Timestamp of host (network byte ordering): 15:31:13 GMT

Information Gathered (26)

3 Exhaustive Web Testing Skipped port 80/tcp

QID:	86718
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/14/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The service aborted the scanning of the Web server before completion, since the Web server stopped responding to HTTP requests during the course

of scanning. The service attempted to reconnect to the Web server two minutes later and found it responsive again. However, the service has chosen to stop further scanning of the Web server to avoid possible interruption of the Web service.

IMPACT:

Since the service did not complete scanning this host, not all vulnerability tests were completed. It's possible that not all vulnerabilities were detected for this host.

SOLUTION:

There may have been a number of conditions that contributed to this issue. The following is a partial list of possibilities that should be investigated:
- The Web server may have reached its connection limit.
- The Web server (or an intervening network device) may have been purposefully throttling connections (e.g. mod_throttle for Apache).
- The Web server (or an intervening network device) may contain an undisclosed Denial of Service condition that was triggered by the scan traffic.
- The Web server (or an intervening network device) may have experienced a degradation of performance due to high load (e.g. via scanning multiple virtual

IPs on the same physical host).
- The scan traffic may have been traversing a network segment with limited bandwidth capacity.
- An Intrusion Prevention System, reactive firewall, or similar device may have detected and blocked the scan traffic.

This issue may possibly be mitigated by modifying the scan performance settings in your option profile before scanning the host again.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The web server stopped responding to 4 consecutive HTTP requests 2 minutes ago. Although it resumed responding to a new HTTP request but the service had terminated further scanning of the web server to avoid interrupting the web server's normal functionality and a prolonged scanning time.

3 Exhaustive Web Testing Skipped

port 443/tcp over SSL

QID:	86718
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/14/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The service aborted the scanning of the Web server before completion, since the Web server stopped responding to HTTP requests during the course

of scanning. The service attempted to reconnect to the Web server two minutes later and found it responsive again. However, the service has chosen to stop further scanning of the Web server to avoid possible interruption of the Web service.

IMPACT:

Since the service did not complete scanning this host, not all vulnerability tests were completed. It's possible that not all vulnerabilities were detected for this host.

SOLUTION:

There may have been a number of conditions that contributed to this issue. The following is a partial list of possibilities that should be investigated:
- The Web server may have reached its connection limit.
- The Web server (or an intervening network device) may have been purposefully throttling connections (e.g. mod_throttle for Apache).
- The Web server (or an intervening network device) may contain an undisclosed Denial of Service condition that was triggered by the scan traffic.
- The Web server (or an intervening network device) may have experienced a degradation of performance due to high load (e.g. via scanning multiple virtual

IPs on the same physical host).
- The scan traffic may have been traversing a network segment with limited bandwidth capacity.
- An Intrusion Prevention System, reactive firewall, or similar device may have detected and blocked the scan traffic.

This issue may possibly be mitigated by modifying the scan performance settings in your option profile before scanning the host again.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The web server stopped responding to 4 consecutive HTTP requests 2 minutes ago. Although it resumed responding to a new HTTP request but the service had terminated further scanning of the web server to avoid interrupting the web server's normal functionality and a prolonged scanning time.

 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/30/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 31 days, 15 hours, and 3 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
3.6.98.232	3946-122-161-74-80.ngrok-free.app
3.6.98.232	ec2-3-6-98-232.ap-south-1.compute.amazonaws.com

1 Firewall Detected

QID:	34011
Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 111, 135, 445, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-21,23-27,29,31,33,35,37-39,41-79,81-223,225,242-246,
256-265,280-282,309,311,318,322-325,340,344-351,363,369-381,383-442,444-581,
587,592-593,598,600,606-620,623-624,626-627,631,633-637,646,666-675,685,
700,704-705,707,709-711,729-731,740-742,744,747-754,758-765,767,769-777,
780-783,786,789,799-801,805-806,808,830,843,860,873,880,886-888,900-902,
911,943,950,954-955,990-1001,1008,1010-1012,1015,1022-1100,1109-1112,
1114,1119,1123,1155,1167,1170,1177,1194,1200,1207,1212,1214,1220-1222,
1234-1236,1241,1243,1245,1248,1250,1269,1290,1311,1313-1314,1337,1344-1625,
1636-1774,1776-1815,1818-1824,1830,1833,1883,1900-1909,1911-1920,1935, and more.
We have omitted from this list 1492 higher ports to keep the report size manageable.

 1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/16/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

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

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: NET-3-6-0-0-1
Network description:
Amazon Data Services India AMAZON-BOM

1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

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

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: APNIC-14
ISP Network description:
Asia Pacific Network Information Centre

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	103.75.173.2	0.13ms	ICMP	
2	14.142.22.253	53.20ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	*.*.*.*	0.00ms	Other	80
5	*.*.*.*	0.00ms	Other	80
6	*.*.*.*	0.00ms	Other	80
7	*.*.*.*	0.00ms	Other	80
8	*.*.*.*	0.00ms	Other	80
9	*.*.*.*	0.00ms	Other	80
10	3.6.98.232	2.70ms	ICMP	

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 854 seconds

Start time: Sun, Apr 06 2025, 15:29:51 GMT

End time: Sun, Apr 06 2025, 15:44:05 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/27/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
3946-122-161-74-80.ngrok-free.app	User-provided DNS

1 Apache HTTP Server Detected

QID:	45391
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/11/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache HTTP Server was detected on the target.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Apache web server detected on port 443 -
Accept-Ranges: bytes
Content-Type: text/html
Date: Sun, 06 Apr 2025 15:35:55 GMT
Etag: "29cf-630eeb1ea0693-gzip"
Last-Modified: Sat, 22 Mar 2025 13:53:25 GMT
Ngrok-Agent-Ips: 122.161.74.80
Server: Apache/2.4.63 (Debian)
Vary: Accept-Encoding

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;
```

```
  background-color: #D8DBE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

div.main_page {
  position: relative;
  display: table;

  width: 800px;

  margin-bottom: 3px;
  margin-left: auto;
  margin-right: auto;
  padding: 0p
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:15:58
TCP	443	0:24:15

1 Open TCP Services List

QID:	82023

Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/19/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

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

SOLUTION:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

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

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

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	15:31:13 GMT

 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 980692252 with a standard deviation of 562328460. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(6255 microseconds). The degree of difficulty to exploit the

TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/28/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

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

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

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 80: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 31 milli seconds

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/11/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/$%7B%28%22QualysQID%22+%2213251%22%29%7D/	web page

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/11/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/icons/	brute force
/javascript/	brute force

1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
ECDHE-ECDSA-AES128-GCM-SHA256	ECDH	ECDSA	AEAD	AESGCM(128)	MEDIUM
TLSv1.3 PROTOCOL IS ENABLED					

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is disabled on the target.
TLSv1.3 session caching is disabled on the target.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

1 SSL Certificate will expire within next six months port 443/tcp over SSL

QID:	38600
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/15/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.ngrok-free.app The certificate will expire within six months: Jul 2 17:10:00 2025 GMT

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/02/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
TLSv1.3						

 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	required
Heartbeat	no
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no

1 Secure Sockets Layer (SSL) Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.ngrok-free.app			
Certificate	no	(unknown)	(unknown)	ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	dddcca3495d7e11605e79532fac79ff83d1c50dfdb003a1412760a2cacbbc82a	Thu 01 Jan 1970 12:00:00 AM GMT

QID:	86002
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/08/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	05:7a:14:39:ca:d1:0f:dd:b6:9f:a5:82:5b:cf:fd:b9:8e:1e
(0)Signature Algorithm	ecdsa-with-SHA384
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E5
(0)SUBJECT NAME	
commonName	*.ngrok-free.app
(0)Valid From	Apr 3 17:10:01 2025 GMT
(0)Valid Till	Jul 2 17:10:00 2025 GMT
(0)Public Key Algorithm	id-ecPublicKey
(0)EC Public Key	
(0)	Public-Key: (256 bit)
(0)	pub:
(0)	04:92:35:6c:ef:d7:de:64:3e:05:40:ae:1d:15:8d:
(0)	d9:06:e8:58:13:f3:71:68:1c:a5:34:fe:ce:6c:3c:
(0)	4a:6c:6e:d4:02:d7:e8:ee:7a:e5:4b:de:4b:77:e5:
(0)	31:7f:91:61:d3:2a:00:48:4a:f0:21:78:51:da:40:
(0)	a8:ef:a1:c4:58
(0)	ASN1 OID: prime256v1
(0)	NIST CURVE: P-256

(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	EB:05:9C:BF:78:3F:6B:49:24:19:1A:14:74:96:DD:27:9C:A0:89:1D
(0)X509v3 Authority Key Identifier	keyid:9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D
(0)Authority Information Access	OCSP - URI:http://e5.o.lencr.org
(0)	CA Issuers - URI:http://e5.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:*.ngrok-free.app, DNS:ngrok-free.app
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://e5.c.lencr.org/31.crl
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : CC:FB:0F:6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C:
(0)	22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0
(0)	Timestamp : Apr 3 18:08:31.913 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:9B:A7:D6:AE:2A:C6:D4:56:D3:C1:88:
(0)	1F:37:0A:CD:B3:E2:9F:B7:BB:7E:D5:F4:FF:5B:00:D9:
(0)	16:02:5E:90:E6:02:20:03:95:8B:7E:4C:92:25:DB:7B:
(0)	71:C4:56:93:E5:AF:15:F1:1D:BA:CB:77:63:37:B8:49:
(0)	6A:7A:02:88:69:2F:18
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : DD:DC:CA:34:95:D7:E1:16:05:E7:95:32:FA:C7:9F:F8:
(0)	3D:1C:50:DF:DB:00:3A:14:12:76:0A:2C:AC:BB:C8:2A
(0)	Timestamp : Apr 3 18:08:31.933 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:AE:A4:89:35:AD:D5:C1:BD:37:36:51:
(0)	97:A6:CF:63:B9:70:70:94:5F:A8:C9:CC:AC:0E:31:0C:
(0)	56:02:FB:E9:AB:02:21:00:8F:1A:2A:59:40:90:69:EC:
(0)	3A:05:A8:ED:41:8D:C1:46:6D:A2:E0:2E:37:85:89:61:
(0)	3A:9B:EB:E5:22:AA:A5:A9
(0)Signature	(103 octets)
(0)	30:65:02:31:00:94:c2:01:06:66:7e:2e:13:61:c6:a5
(0)	42:13:45:de:d5:c5:af:ce:1a:b1:3b:d6:5e:af:ec:85
(0)	e7:d2:34:b8:b5:91:4c:9b:b7:ff:42:82:73:78:32:da
(0)	85:27:15:9d:8b:02:30:1f:8a:1d:fe:2b:7d:c5:fa:1c
(0)	57:46:9b:d8:04:81:7d:65:33:2e:bc:e8:79:9c:f9:fa
(0)	c1:66:45:e7:59:96:ea:c8:44:db:61:4a:d3:a3:04:54
(0)	87:f8:ea:6b:fe:60:39:6e
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	83:8f:6c:63:ce:b1:39:8c:62:06:62:83:15:c9:fd:de
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1

(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E5
(1)Valid From	Mar 13 00:00:00 2024 GMT
(1)Valid Till	Mar 12 23:59:59 2027 GMT
(1)Public Key Algorithm	id-ecPublicKey
(1)EC Public Key	
(1)	Public-Key: (384 bit)
(1)	pub:
(1)	04:0d:0b:3a:8a:6b:61:8e:b6:ef:dc:5f:58:e7:c6:
(1)	42:45:54:ab:63:f6:66:61:48:0a:2e:59:75:b4:81:
(1)	02:37:50:b7:3f:16:79:dc:98:ec:a1:28:97:72:20:
(1)	1c:2c:cf:d5:7c:52:20:4e:54:78:5b:84:14:6b:c0:
(1)	90:ae:85:ec:c0:51:41:3c:5a:87:7f:06:4d:d4:fe:
(1)	60:d1:fa:6c:2d:e1:7d:95:10:88:a2:08:54:0f:99:
(1)	1a:4c:e6:ea:0a:ac:d8
(1)	ASN1 OID: secp384r1
(1)	NIST CURVE: P-384
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D
(1)X509v3 Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)Signature	(512 octets)
(1)	1f:72:9d:34:45:42:41:da:a4:d0:b2:b2:b8:d2:26:4c
(1)	a7:51:25:8d:42:da:ec:36:48:96:a3:ba:1a:a4:c8:63
(1)	d8:f0:2f:b3:ce:cb:9f:67:e9:a0:9e:19:ea:d4:0d:8a
(1)	55:03:92:ca:43:84:9d:46:f1:d5:cc:ba:df:ba:c1:02
(1)	28:71:f7:ba:fe:6d:cc:1b:64:ce:ac:4c:32:1a:12:b8
(1)	91:fc:f2:e4:e8:b2:ac:f4:17:b4:ba:85:71:80:e2:83
(1)	72:91:bd:b2:f0:f7:dc:9f:86:f4:b7:1f:bf:52:bd:96
(1)	e0:e6:49:38:06:e9:73:45:20:de:6f:7c:8e:60:b3:f9
(1)	4c:3f:2a:23:10:c7:48:cc:af:5b:95:c9:76:ff:5b:ca
(1)	c4:ef:16:18:27:23:be:c4:35:9c:9f:cf:c2:df:0b:41
(1)	90:5f:38:5c:95:5c:ff:2e:6c:0a:7f:6a:ed:dd:73:81
(1)	0a:58:6f:4c:3b:9c:dc:c7:5a:93:f7:e3:57:44:67:55
(1)	5b:11:af:98:11:51:01:a8:dc:88:c7:d7:30:4d:59:b8
(1)	69:a4:df:f1:8e:92:80:0c:ed:99:23:66:69:5e:ca:89
(1)	0f:d4:b1:b3:99:f2:5c:51:df:6c:ed:e7:ae:d7:ff:7f
(1)	7a:0e:57:95:77:7f:e7:91:ad:62:30:0c:f8:2e:03:1b
(1)	98:bb:79:a3:6a:72:6d:85:fb:2c:58:20:fb:7a:71:b6
(1)	ed:61:53:49:08:67:c7:5a:a1:c4:43:81:58:4a:d5:32
(1)	16:7b:fc:b2:3c:aa:53:cc:a9:81:96:8d:27:d6:95:71
(1)	64:88:08:b3:88:13:5f:d0:bf:fe:e8:2a:c9:d9:09:62
(1)	7d:db:ac:14:e9:1a:86:d4:e6:0f:18:e8:b5:ce:e0:01
(1)	84:bc:3a:d5:cb:8f:54:34:f6:f2:74:12:fd:ee:b3:f7

(1)	97:09:5e:ad:1e:2b:50:5c:68:9e:9f:25:9b:26:6e:34
(1)	60:0f:9a:77:9a:f1:1f:e6:f7:50:33:b3:02:12:f5:34
(1)	b4:76:ec:c7:62:39:98:71:c9:a0:00:47:6f:c2:95:06
(1)	05:a9:fe:57:17:19:68:96:69:e3:b2:07:b4:4f:f8:e7
(1)	c3:b6:f8:b6:3a:c6:a9:c5:78:95:ee:f3:55:b3:b7:cc
(1)	96:b4:63:63:58:e8:29:aa:a6:9b:27:27:06:f0:2a:d7
(1)	80:04:6e:dc:8b:b1:57:ce:4b:ae:81:f1:aa:64:78:55
(1)	f6:35:8e:17:3c:46:15:e1:94:82:7b:c5:47:3e:b7:6b
(1)	11:19:36:c0:82:c6:dd:3f:c4:1a:64:88:90:26:15:50
(1)	c4:a7:8e:62:5d:55:00:fd:17:a3:5a:ff:ec:e6:5c:27

Appendix

Hosts Scanned (DNS)

3946-122-161-74-80.ngrok-free.app

Options Profile

Qualys Recommended Option Profile

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Close Vulnerabilities on Dead Hosts Count:	Off
Purge old host data when OS changes:	On
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Maximum Scan Duration per Asset:	
Maximum Scan Duration Per Asset:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco/Network SSH:	Enabled
Unix Least Privilege Authentication:	Enabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled

NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Cassandra:	Disabled
MarkLogic:	Disabled
DataStax:	Disabled
Overall Performance:	Normal
Allow Parallel Scanning:	Disabled
Limit Per Host CGI Checks:	disabled
Configure Scan for Limited Connectivity:	disabled
Set Maximum Targets per Slice:	disabled
Skip Pre-scanning:	disabled
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	On
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Enabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

System Authentication

System Authentication Records:

Include system created authentication records in scans: Disabled

Advanced Settings

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

Report Legend

Vulnerability Levels

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

Severity	Level	Description

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

Potential Vulnerability Levels

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

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

Information Gathered

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

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

This report was generated with an evaluation version of Qualys