Vulnerability Report

Scan name:	b2283948-cbe8-45e7-b291-45f69620596d
Host(s) scanned:	AA.sample.com
Date and time:	2023-04-21 06:08:22
Standard:	PCI

Table of Contents

Report Summary

Scan name:	b2283948-cbe8-45e7-b291-45f69620596d
Host(s) scanned:	AA.sample.com
Date and time:	2023-04-21 06:08:22

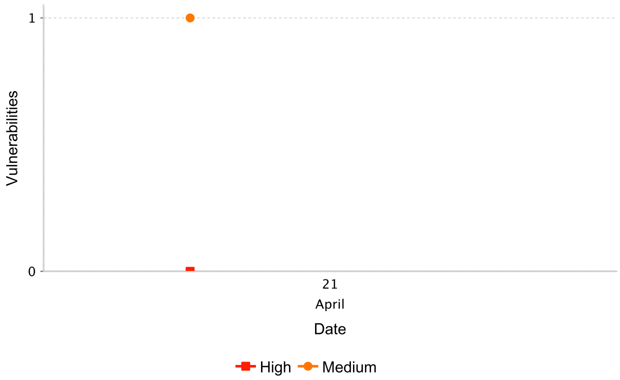
Time to finish: 07 minutes and 19 seconds to complete.

The 'Possible Vulnerabilities' section of this report lists security holes found during the scan, sorted by risk level. Note that some of these reported vulnerabilities could be 'false alarms' since the hole is never actually exploited during the scan.

Some of what we found is purely informational; It will not help an attacker to gain access, but it will give him information about the local network or hosts. These results appear in the 'Low risk / Intelligence Gathering' section.

Vulnerability Trend

High and Medium Risk totals discovered on scan 'b2283948-cbe8-45e7-b291-45f69620596d' and their change in number over time.



Remediation Focus

Repair the most common security issues on scan 'b2283948-cbe8-45e7-b291-45f69620596d' and 100% of its vulnerabilities will be resolved.

Applying
1
Top Remediations

Will Remediate
100%
Vulnerabilities

Affecting
1
Hosts

Top 1 remediations

1. SSH Supports Weak Algorithms

Executive Summary

Overview

Scan Name	Total	High	Medium	Low	Score *
b2283948-cbe8-45e7-b291-45f69620596d	8	0	1	7	90.00

Vulnerabilities by Host and Risk Level

Host	Total	High	Medium	Low	Score	PCI
AA.sample.com	8	0	1	7	90.00	No
Number of host(s): 1						

Vulnerabilities by Service and Risk Level

Service	Total	High	Medium	Low	Score *
general (icmp)	1	0	0	1	100.00
general (tcp)	2	0	0	2	100.00
ssh (22/tcp)	2	0	1	1	90.00
http (80/tcp)	2	0	0	2	100.00
ntp (123/udp)	1	0	0	1	100.00

Vulnerabilities by Category

Category	Total	High	Medium	Low	Score *
SSH servers	1	0	1	0	90.00
Network devices	1	0	0	1	100.00
Simple Network services	1	0	0	1	100.00
Web servers	1	0	0	1	100.00
Preliminary Analysis	4	0	0	4	100.00

* The vulnerability score indicates the host's difficulty to hack on a scale from 0 to 100.
0 is very easy to gain unauthorized access, like easily exploited vulnerabilities or many potential unauthorized access points on the host.
100 is very difficult to gain unauthorized access, with no known vulnerabilities or only low risk vulnerabilities.

Executive Summary

Vulnerabilities in the report are classified into 3 categories: high, medium or low. This classification is based on industry standards and is endorsed by the major credit card companies. The following is the categories definitions:

High Risk Vulnerability

are defined as being in one or more of the following categories: Backdoors, full Read/ Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords)

Medium Risk Vulnerability

are vulnerabilities that are not categorized as high risk, and belong to one or more of the following categories: Limited Access to files on the host, Directory Browsing and Traversal, Disclosure of Security Mechanisms (Filtering rules and security mechanisms), Denial of service, Unauthorized use of services (e.g. Mail relay).

Low Risk Vulnerability

are those that do not fall in the "high" or "medium" categories. Specifically, those will usually be: Sensitive information gathered on the server's configuration, Informative tests.

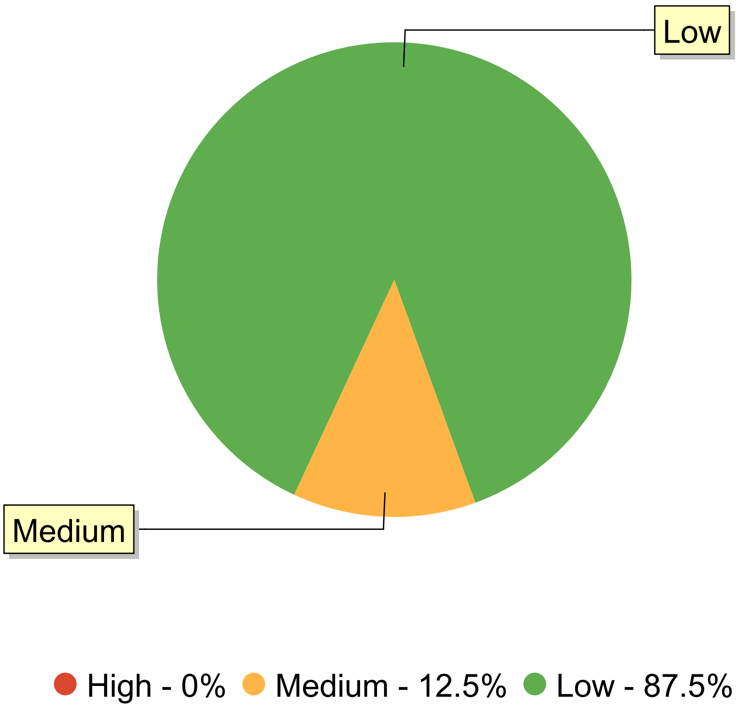
Other Issues

Host information - provided by different tests that discover information about the target host, results of those test are not classified as vulnerabilities.

Guessed Platform - Detection of the operation system running on the host, via TCP/IP Stack FingerPrinting, this test is not very accurate, thus it is guessing.

Possible Vulnerabilities

Vulnerabilities Breakdown by Risk



1. SSH SUPPORTS WEAK ALGORITHMS / SSH servers

Host(s) affected:

AA.sample.com: ssh (22/tcp)

PCI Compliance Status: Fail

Summary

The remote SSH server is configured to use weak cipher, mac, kex and hka algorithms.

md.winthecustomer.com : ssh (22/tcp)

```
Weak mac algorithms was found in SSH Server:
hmac-sha1, umac-64, hmac-sha1-etm@openssh.com, umac-64-etm@openssh.com

Weak kex algorithms was found in SSH Server:
diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

Weak hka algorithms was found in SSH Server:
ecdsa-sha2-nistp256
```

Possible Solution

If you are using OpenSSH 6.7 and newer you can use the following SSH configuration directives to strengthen the SSH security:

```
# Specifies the available KEX (Key Exchange) algorithms.
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256

# Specifies the ciphers allowed.
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

#Specifies the available MAC (message authentication code) algorithms.
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128
```

Risk: Medium

CVSS Score: 4.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

OWASP: A9

More Information

https://stribika.github.io/2015/01/04/secure-secure-shell.html, https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html

TestID: 19804 (Revision: 3, Added: 2018-09-25)

1. ICMP TIMESTAMP REQUEST / Preliminary Analysis

Host(s) affected:
AA.sample.com: general (icmp)
PCI Compliance Status: Pass

Summary
The remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.

Impact
This may help attackers to defeat time based authentications schemes.

Possible Solution
See solution provided at: https://beyondsecurity.zendesk.com/hc/en-us/articles/203609549--How-can-I-mitigate-ICMP-Timestamp-

Risk: Low

CVSS Score: 0.00

OWASP: A6

CVSS Score: 0.00

CVSS: AV:L/AC:L/Au:N/C:N/I:N/A:N

CVE: CVE-1999-0524

Microsoft Knowledge Base: 313190

More Information
http://www.beyondsecurity.com/faq/questions/54/how-can-i-mitigate-icmp-timestamp, https://beyondsecurity.zendesk.com/hc/en-us/articles/203609549--How-can-I-mitigate-ICMP-Timestamp-, https://social.technet.microsoft.com/Forums/windows/en-US/219f3dcc-3e5b-4d9b-88ae-137215575c7f/icmp-timestamp-response?forum=w7itprosecurity

TestID: 811 (Revision: 6, Added: 2000-01-01)

2. NTP VARIABLES READING / Simple Network services

Host(s) affected:
AA.sample.com: ntp (123/udp)
PCI Compliance Status: Pass

Summary

It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings.

Theoretically one could work out the NTP peer relationships and track back network settings from this.

md.winthecustomer.com : ntp (123/udp)

Impact

Attackers can gain critical information about the host.

Possible Solution

Set NTP to restrict default access to ignore all info packets: restrict default ignore

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 1653 (Revision: 2, Added: 2000-01-01)

3. TTL ANOMALY DETECTION / Network devices

Host(s) affected:

AA.sample.com: general (tcp)

PCI Compliance Status: Pass

Summary

The remote host, when queried on open ports, replies with differing TTL values. This could be an indicator that a transparent proxy is on the way, or that this host is a forwarding router, honeypot, etc...

Impact

An attacker may use this information to find critical systems on your network.

Possible Solution

Contact vendor for information on closing up this information leak.

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 2711 (Revision: 1, Added: 2003-10-16)

4. IDENTIFY UNKNOWN SERVICES VIA GET REQUESTS / Preliminary Analysis

Host(s) affected:
AA.sample.com: http (80/tcp) ssh (22/tcp)
PCI Compliance Status: Pass

Summary
This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

AA.sample.com : http (80/tcp)

```
A web server is running on this port
```

md.winthecustomer.com : ssh (22/tcp)

```
A SSH server is running on this port
```

Risk: Low

CVSS Score: 1.00*
Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system
TestID: 8434 (Revision: 2, Added: 2005-04-06)

5. HTTP PACKET INSPECTION / Web servers

Host(s) affected:
md.winthecustomer.com: http (80/tcp)
PCI Compliance Status: Pass

Summary
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.

md.winthecustomer.com : http (80/tcp)

```
Protocol version: HTTP/1.1
SSL: no
Pipelining: no
Keep-Alive: no
Options allowed: (Not implemented)
Headers:
```

```
Server: nginx/1.14.2

Date: Fri, 21 Apr 2023 06:04:48 GMT

Content-Type: text/html

Content-Length: 3643

Last-Modified: Mon, 29 Jan 2018 17:32:35 GMT

Connection: close

ETag: "5a6f5ab3-e3b"

Accept-Ranges: bytes
```

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 10209 (Revision: 1, Added: 2007-02-08)

6. TCP TIMESTAMPS RETRIEVAL / Preliminary Analysis

Host(s) affected:

AA.sample.com: general (tcp)

PCI Compliance Status: Pass

Summary

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can be sometimes be computed.

md.winthecustomer.com : general (tcp)

```
The uptime was estimated to 1011991s, i.e. about 11 days.
(Note that the clock is running at about 1000 Hz and will overflow in about 4294964s, that is 49 days)
```

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

OWASP: A6

More Information

http://www.ietf.org/rfc/rfc1323.txt

TestID: 10399 (Revision: 1, Added: 2007-05-27)

Host Information

Information about host: md.winthecustomer.com

OS Detection:
md.winthecustomer.com

TestID: 2907
Nmap found that this host has an uptime of 11.712 days

TestID: 1043
Scanner IP: 10.0.201.248
Target IP: 157.230.67.179
Target Hostname: md.winthecustomer.com

TestID: 9162

general (icmp): Port found open

ssh (22/tcp):
An ssh server is running on this port

TestID: 772

SSH version: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1

TestID: 942
The remote SSH daemon supports the following versions of the SSH protocol:

. 1.99
. 2.0

SSHv2 host key fingerprint : c4:10:3f:12:2d:27:67:7c:9d:b1:44:ca:e1:39:4a:66

TestID: 1642

http (80/tcp):
A web server is running on this port

TestID: 772
nginx/1.14.2

TestID: 1035