Automated Vulnerability Scan Results

Table of Contents

Introduction

The '**www.example.com**' scan has been completed.
You requested a report of the following host(s): **www.example.com**.
The scan took place on **2013-10-30 14:55:12** (Scan Number: 1).

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.

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 vulnerabilities

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 vulnerabilities

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 vulnerabilities

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.

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.

Top Level Overview

Scan	Total	High	Medium	Low
www.example.com	7	0	0	7

Vulnerabilities by Host and Risk Level

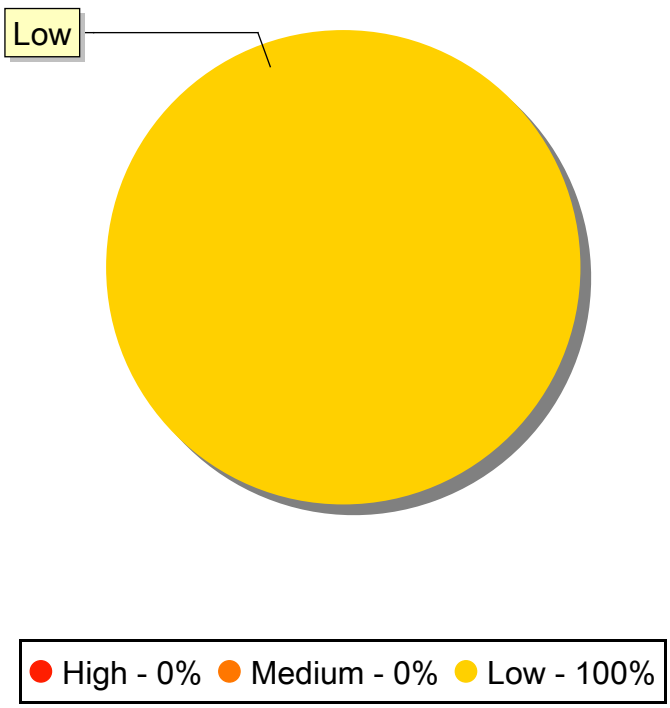
Host	Total	High	Medium	Low
www.example.com	7	0	0	7
Number of host(s): 1				

Vulnerabilities by Service and Risk Level				
Service	Total	High	Medium	Low
general (udp)	1	0	0	1
http (80/tcp)	2	0	0	2
https (443/tcp)	4	0	0	4

Vulnerabilities by Category				
Family	Total	High	Medium	Low
Encryption and Authentication	2	0	0	2
Web servers	4	0	0	4
Firewalls	1	0	0	1

Possible Vulnerabilities

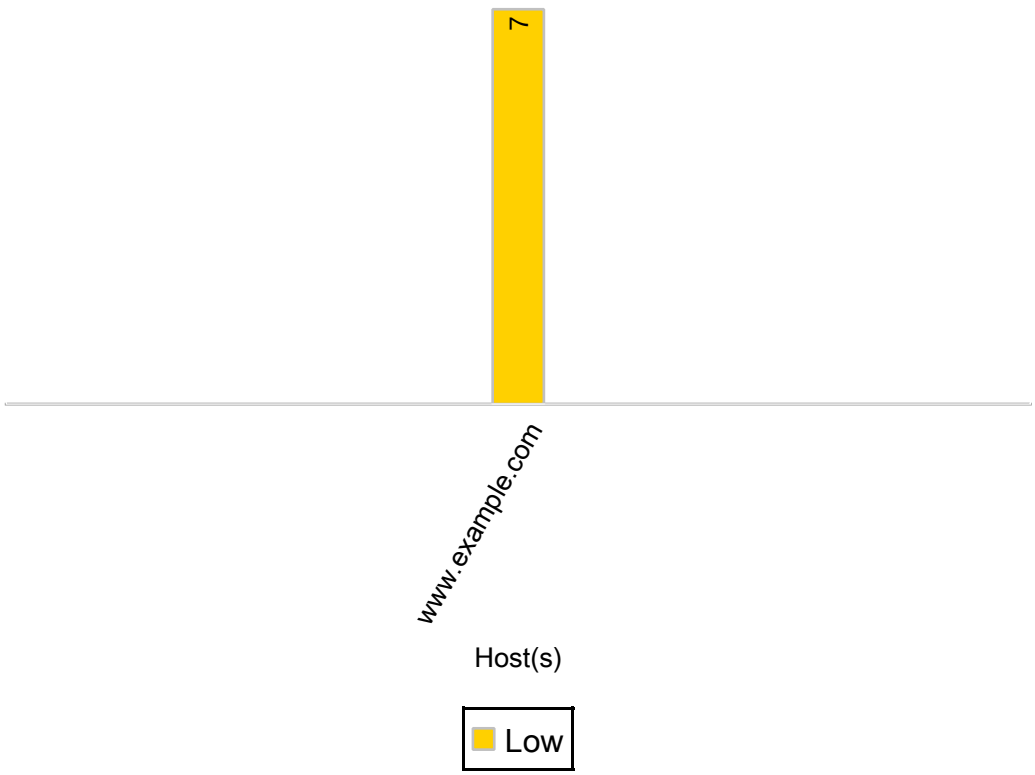
Vulnerabilities Breakdown by Risk



Low

7 Low risk vulnerabilities were discovered (5 Unique)

Top Vulnerable Hosts (Low)



1. HTTP TRACE

Web servers

Host(s) affected:

www.example.com : http (80/tcp) https (443/tcp)

We tried to discover any HTTP proxies (or reverse proxies) that are on the route to the host.

www.example.com:

There might be a caching proxy on the way to this web server

www.example.com:

There might be a caching proxy on the way to this web server

Impact:

This is not a security hole, only an intelligence gathering.

TestID:1831 (Revision: 1, Added: 2002-07-04)

2. DNS Bypass Firewall Rules (UDP 53)

Firewalls

Host(s) affected:

www.example.com : general (udp)

It is possible to by-pass the rules of the remote firewall by sending UDP packets with a source port equal to 53.

An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall.

Possible Solution:

Review your Firewall rules policy.

CVSS Score: 5.00

CVSS:

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

CVE:

CVE-2004-1473

TestID:2257 (Revision: 1, Added: 2003-06-03)

3. SSL Verification Test

Encryption and Authentication

Host(s) affected:

www.example.com : https (443/tcp)

This test connects to a SSL server, and checks its certificate and the available (shared) SSLv2 ciphers. Weak (export version) ciphers are reported as problematic.

www.example.com:
Here is the SSLv3 server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
06:2d:48:89:86:c9:a6:d7:f9:49:01:c2:b5:90:68:82
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance CA-3
Validity
Not Before: Oct 3 00:00:00 2011 GMT
Not After : Dec 10 12:00:00 2014 GMT
Subject: C=US, ST=California, L=Santa Monica, O=EdgeCast Networks, Inc., CN=gp1.wac.edgecastcdn.net
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:b8:ae:55:d6:71:a8:09:13:cb:33:fe:df:38:ce:
10:2f:7b:ef:f5:6f:bb:7b:a1:ac:de:5b:f2:32:84:
cb:df:38:9e:ab:3b:80:1a:9c:8c:f4:2b:3b:bd:1b:
f6:83:fa:d9:e3:d9:76:2a:0c:db:34:af:7e:24:87:
9e:d0:b0:b6:71:31:5b:42:e1:3d:0d:a5:57:44:62:
e8:f1:d0:21:9c:fd:1c:14:c6:c4:ad:cc:5e:85:67:
58:da:e2:2d:97:94:5d:c4:6c:c1:60:fb:ce:4c:c0:
45:a4:b8:33:aa:3a:aa:bc:dd:1a:b9:32:34:21:86:
ec:cc:4e:06:21:c2:50:42:6e:84:9d:3e:3f:79:0d:
c5:54:2a:c3:a3:6e:a3:e2:2b:63:f1:53:fe:8c:1b:
f2:a7:33:dd:a1:39:92:09:b4:40:05:ca:77:d0:84:
0f:b1:5d:24:b7:51:cc:f0:e3:72:68:c3:64:ef:ec:
f1:e4:e1:cb:b8:16:d2:29:cc:85:9a:f7:64:89:3e:
16:c7:bf:d0:dd:d0:61:e5:1c:7d:d6:e4:e8:20:1a:
05:22:07:a0:96:64:b7:3b:8f:ea:3e:74:1d:81:0c:
97:1c:03:ff:82:73:0a:03:4d:1a:63:ba:95:27:9e:
0d:ae:ac:41:93:bf:c2:f0:6d:44:5e:c0:03:a6:54:
f9:83
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:50:EA:73:89:DB:29:FB:10:8F:9E:E5:01:20:D4:DE:79:99:48:83:F7

X509v3 Subject Key Identifier:
34:3A:FB:35:2B:21:FA:38:24:B5:E6:75:28:A0:FD:28:65:F0:27:9D
X509v3 Subject Alternative Name:
DNS:gp1.wac.edgecastcdn.net, DNS:www.edgecast.com, DNS:wac.edgecastcdn.net, DNS:ne.wac.edgecastcdn.net, DNS:swf.mixpo.com, DNS:cdn.traceregister.com, DNS:s.tmocache.com, DNS:s.my.tmocache.com, DNS:e1.boxcdn.net,

DNS:e2.boxcdn.net, DNS:e3.boxcdn.net, DNS:www.sonos.com, DNS:static-cache.tp-global.net, DNS:ssl-cdn.sometrics.com, DNS:cache.vehicleassets.captivelead.com, DNS:static.woopra.com, DNS:images.ink2.com, DNS:assets-secure.razoo.com, DNS:ec.pond5.com, DNS:images.esellerpro.com, DNS:use.typekit.com, DNS:static.iseatz.com, DNS:static.www.turnto.com, DNS:inpath-static.iseatz.com, DNS:secure.avelleassets.com, DNS:static.dubli.com, DNS:www-cdn.cinamuse.com, DNS:www-cdn.cineble.com, DNS:www-cdn.cinemaden.com, DNS:www-cdn.filmlush.com, DNS:www-cdn.flixaddict.com, DNS:www-cdn.itshd.com, DNS:www-cdn.moviease.com, DNS:www-cdn.movielush.com, DNS:www-cdn.reelhd.com, DNS:www-cdn.pushplay.com, DNS:cdn1.fishpond.co.nz, DNS:cdn1.fishpond.com.au, DNS:www.isaca.org, DNS:cdn.optimizely.com, DNS:static.shoedazzle.com, DNS:www.travelrepublic.co.uk, DNS:cdn.nprove.com, DNS:sslbest.booztx.com, DNS:www.travelrepublic.com, DNS:www.blacklabelads.com, DNS:cdn.whois.com.au, DNS:ne1.wac.edgecastcdn.net, DNS:gs1.wac.edgecastcdn.net, DNS:c1.socialcastcontent.com, DNS:www.steepandcheap.com, DNS:www.whiskeymilitia.com, DNS:www.chainlove.com, DNS:www.tramdock.com, DNS:www.bonktown.com, DNS:www.brociety.com, DNS:edgecast.onegrp.com, DNS:cdn.psw.net, DNS:cdn.gaggle.net, DNS:www-cdn.reelvidz.com, DNS:fast.fonts.com, DNS:ec.xnglobalres.com, DNS:images.vrbo.com, DNS:beta.fileblaze.net, DNS:cdn.brandsexclusive.com.au, DNS:www-cdn.ireel.com, DNS:cdcssl.ibsrv.net, DNS:cdn.betchoice.com, DNS:player.vzaar.com, DNS:framegrabs.vzaar.com, DNS:thumbs.vzaar.com, DNS:stylistlounge.stelladot.com, DNS:www.stelladot.com, DNS:content.aqcdn.com, DNS:content.ebgames.com.au, DNS:content.ebgames.co.nz, DNS:images.pagerage.com, DNS:images.allsaints.com, DNS:cdnb1.kodakgallery.com, DNS:cdn.orbengine.com, DNS:cdn.quickoffice.com, DNS:content.glscrip.com, DNS:cdn.bidfan.com, DNS:media.quantumads.com, DNS:cdn.allenbrothers.com, DNS:pics.intelius.com, DNS:pics.peoplelookup.com, DNS:pics.lookupanyone.com, DNS:cdn1-ssl.iha.com, DNS:s.cdn-care.com, DNS:cdn2-b.examiner.com, DNS:cdn.trtk.net, DNS:edgecdn.ink2.com, DNS:ec.dstimage.disposolutions.com, DNS:cdn.clytel.com, DNS:welcome2.carsdirect.com, DNS:s1.card-images.com, DNS:update.alot.com, DNS:www.outsystems.com, DNS:www.drwmedia.com, DNS:lookup.bluecava.com, DNS:cdn.taxact.com, DNS:cdn.taxactonline.com, DNS:cdn.200581.com, DNS:img.vxcdn.com, DNS:js.vxcdn.com, DNS:www.goal.com, DNS:cdns1.kodakgallery.com, DNS:edge.dropdowndeals.com, DNS:edge.pagerage.com, DNS:edge.sanityswitch.com, DNS:edge.yontoo.com, DNS:layers.yontoo.com, DNS:cdn.widgetserver.com, DNS:www.cloudwords.com, DNS:edge.actaads.com, DNS:images.skincarerx.com, DNS:ssl.cdn-redfin.com, DNS:small.outso-media.com, DNS:cdn.foxycart.com, DNS:edge.jeetyetmedia.com, DNS:cdn.ticketfly.com, DNS:images.cosmeticmall.com, DNS:www.backcountry.com, DNS:ssl.booztx.com, DNS:p.typekit.net, DNS:use.typekit.net, DNS:cdn.thewatershed.com, DNS:www.sf-cdn.net, DNS:static.cdn.dollarsdirect.com.au, DNS:edge.redfordmediallc.com, DNS:edge.pluralmediallc.com, DNS:www.gourmetgiftbaskets.com, DNS:www.numberinvestigator.com, DNS:b2bportal.disneylandparis.com, DNS:b2bportal.disneytravelagents.co.uk, DNS:www.nwf.org, DNS:assets.zendesk.com, DNS:a.cdnkic.com, DNS:s.cdnkic.com, DNS:www.superbiketoystore.com, DNS:cdn.stylethread.com.au, DNS:cdn.cartrawler.com, DNS:publicstaticcdn.tableausoftware.com, DNS:secure.33across.com, DNS:c.ztstatic.com, DNS:c.mscimg.com, DNS:static.teamtreehouse.com, DNS:wac.A8B5.edgecastcdn.net
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 CRL Distribution Points:
URI:http://crl3.digicert.com/ca3-g23.crl
URI:http://crl4.digicert.com/ca3-g23.crl

X509v3 Certificate Policies:
Policy: 2.16.840.1.114412.1.1
CPS: http://www.digicert.com/ssl-cps-repository.htm
User Notice:
Explicit Text:

Authority Information Access:
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertHighAssuranceCA-3.crt

X509v3 Basic Constraints: critical
CA:FALSE
Signature Algorithm: sha1WithRSAEncryption

1b:04:c0:dd:6b:22:a7:84:75:d6:22:ce:96:65:26:3c:5e:12:
9d:60:53:7d:91:18:03:50:27:17:4e:79:a5:41:d1:b1:15:47:
b7:e7:d6:b0:9d:24:57:e4:5a:55:f5:6b:da:4f:9c:bd:33:8a:
da:06:4e:b1:f7:27:6f:29:a4:76:d6:e9:af:de:c1:3f:34:0c:
41:07:52:c4:d6:40:4b:df:fa:c3:02:62:48:fc:64:13:28:23:
35:f8:4f:32:6b:3c:72:bd:27:11:8d:69:f4:a3:ed:c5:7c:9b:
3a:9a:df:da:fa:ee:96:89:9e:98:f7:fa:d5:fe:71:70:8e:d2:
4c:23:7b:3f:8c:f4:0e:ce:44:f8:e1:39:8e:c0:a7:f4:29:5c:
4b:5d:85:c3:d3:7e:23:ed:22:c6:55:b5:1d:33:ab:f7:a8:6c:
d4:8d:70:ba:6e:6f:fd:94:03:06:88:09:7a:8e:bd:b2:b2:25:
8d:0f:0a:f1:38:91:7e:b9:01:68:7f:31:a2:63:f8:f7:22:d3:
3a:1c:65:37:63:7d:a0:76:f5:1e:03:81:70:a4:a6:1f:39:26:
0f:ef:89:86:7d:da:c7:fb:67:d2:99:e1:b5:1d:e4:44:4e:6b:
bc:8e:f9:4f:69:d2:99:59:f5:5f:2e:6b:8d:d9:d0:ad:d3:5f:
9e:88:a8:b6
This TLSv1 server does not accept SSLv2 connections.
This TLSv1 server also accepts SSLv3 connections.

Possible Solution:
Usage of weak ciphers should be avoided.

TestID:2804 (Revision: 3, Added: 2003-12-25)

4. Supported SSL Ciphers Suites | Encryption and Authentication

Host(s) affected:

www.example.com : https (443/tcp)

This test detects which SSL ciphers are supported by remote service for encrypting communications.

www.example.com:

Here is the list of SSL ciphers supported by the remote server:

- High Strength Ciphers (>= 112-bit key)
* SSLv3 - DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
* SSLv3 - RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
* SSLv3 - RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
* TLSv1 - DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
* TLSv1 - AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
* TLSv1 - AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
* TLSv1 - RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
* TLSv1 - RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
* TLSv1 - n/a Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1

The fields above are:

* {OpenSSL ciphername}
* Kx={key exchange}
* Au={authentication}
* Enc={symmetric encryption method}
* Mac={message authentication code}
* {export flag}

More Information:

http://www.openssl.org/docs/apps/ciphers.html

TestID:9819 (Revision: 2, Added: 2006-06-26)

5. HTTP Packet Inspection

Web servers

Host(s) affected:

www.example.com : http (80/tcp) https (443/tcp)

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

www.example.com:
Protocol version: HTTP/1.1
SSL: no
Pipelining: yes
Keep-Alive: no
Options allowed: OPTIONS, GET, HEAD, POST
Headers:

Accept-Ranges: bytes

Cache-Control: max-age=604800

Content-Type: text/html

Date: Wed, 30 Oct 2013 14:35:37 GMT

Etag: "359670651"

Expires: Wed, 06 Nov 2013 14:35:37 GMT

Last-Modified: Fri, 09 Aug 2013 23:54:35 GMT

Server: ECS (iad/1984)

X-Cache: HIT

x-ec-custom-error: 1

Content-Length: 1270

www.example.com:
Protocol version: HTTP/1.1
SSL: yes
Pipelining: yes
Keep-Alive: no
Options allowed: OPTIONS, GET, HEAD, POST
Headers:

Accept-Ranges: bytes

Cache-Control: max-age=604800

Content-Type: text/html

Date: Wed, 30 Oct 2013 14:35:38 GMT

Etag: "359670651"

Expires: Wed, 06 Nov 2013 14:35:38 GMT

Last-Modified: Fri, 09 Aug 2013 23:54:35 GMT

Server: ECS (iad/19C2)

X-Cache: HIT

x-ec-custom-error: 1

Content-Length: 1270

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

Host Information

OS Type Breakdown

No OS available - Insufficient data

Information about host: www.example.com

Host Fully Qualified Domain Name

Scanner IP: 10.224.39.34
Target IP: 93.184.216.119
Target Hostname: www.example.com
Backports: no

TestID:9162
www.example.com
TestID:2907

http (80/tcp)

A web server is running on this port
TestID:772

https (443/tcp)

A TLSv1 server answered on this port

TestID:772
A web server is running on this port through SSL
TestID:772

What Next ?

Knowing is just half the battle. Now you have to go and fix the problems we reported above.
Intelligence gathering attacks may give attackers a good lead when trying to break into your host.
Denial-of-Service attacks are much more dangerous than they seem at first glance, for more information take a look at:

http://www.securiteam.com/securitynews/2JUQ6QAQTE.html

High risk vulnerabilities should be dealt with immediately. They give an attacker almost immediate access to your system! This is also a good time to review your logs and see if you could have identified this scan if it was performed without your knowledge. Conduct these penetration tests periodically to check for the newest attacks.

DISCLAIMER: This report is not meant as an exhaustive analysis of the level of security now present on the tested host, and the data shown here should not be used exclusively to judge the security level of any computer system. The scan was performed automatically, and unlike a manual penetration test it does not reveal all the possible security holes present in the system. Some vulnerabilities that were found might be 'false alarms'. The information in this report is provided "as is" and no liability for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages will be accepted.