

Table Of Contents

Table Of Contents 1

But how do I find out if my DNS server is open to such attack or not? 2

[Home](#) > [Faq](#) > [Bind dns](#)

Find Out If My DNS Server Free From DNS Cache Poisoning Bug Or Not

Posted by [Vivek Gite](#) <vivek@nixcraft.com>

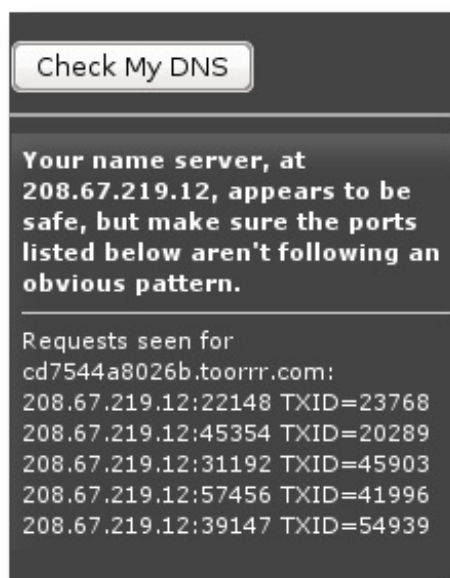
Q. How do I verify that my ISP or my own recursive resolvers are free from DNS cache poisoning bug that is promised full disclosure of the flaw by Dan on August 7 at the Black Hat conference? How do I test my dns server for DNS cache pollution or DNS Cache Poisoning bug?

A. DNS cache poisoning (also known as DNS cache pollution) is a maliciously created or unintended situation that provides data to a Domain Name Server that did not originate from authoritative DNS sources. It occur if DNS "spoofing attack" has been encountered. An attacker will send malicious data / non-secure data in response to a DNS query. For example dns query for www.cyberciti.biz can be redirected to www.example.com.



[1]

But how do I find out if my DNS server is open to such attack or not?

Visit Dan Kaminsky java script page to [check your DNS](#) [2]

[3]

You can also use following command dig command, enter:

```
$ dig +short @{name-server-ip} porttest.dns-oarc.net txt
$ dig +short @ns1.example.com porttest.dns-oarc.net txt
$ dig +short @208.67.222.222 porttest.dns-oarc.net txt
```

Sample output:

```
z.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"208.67.222.222 is GOOD: 26 queries in 0.1 seconds from 26 ports with std dev 17746.18"
```

Another test,

```
$ dig +short @125.22.47.125 porttest.dns-oarc.net txt
```

Output:

```
z.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"125.22.47.139 is POOR: 42 queries in 8.4 seconds from 1 ports with std dev 0.00"
```

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/dns-cache-poisoning-test/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/faq/category/troubleshooting/>

[2] check your DNS: <http://www.doxpara.com/>

[3] Image: <http://www.cyberciti.biz/faq/wp-content/uploads/2008/07/dns-cache-poisoning-test.png>

Copyright © 2006-2010 [nixCraft](#). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.