DNS解析咋就这么多故障计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_DNS_E8_A7_A3_E6_9E_90_E5_c98_644216.htm DNS系统出现故障，大批域名无法正常管理。从5.19到商务中国，到瑞典“ .se ”，到群英QYDNS，再到今天的“ NEW ”，一个接一个，网络世界里的湖面好像从未平静过。是风不甘于平庸，还是水不甘于寂寞？ 总之问题出现了，是别人攻了进来，而且还不只一次。DNS解析故障只是一个手段，就攻击DNS个体而言实在没多大意义，搞瘫DNS目的在于隔断目标与外界的联系，然后再痛下杀手。对入侵者来说他们踩在脚下的是路，是康庄大道，对于受害者来说而是遮不严盖不紧的漏洞。这是才是事故频发的首要原因，黑客利用DNS漏洞来毒害DNS服务器的缓存，将合法的互联网地址取代为有毒害的地址，那么，当你输入银行名字或者其他网站地址，就会被路由到你毫不知情的诈骗网站，对这些来说，断网带来的危害就不算什么了。苍蝇不盯无缝的蛋，入侵者只要找到复杂的计算机网络中的一个缝，就能轻而易举地闯入系统。所以，了解这些缝都有可能在哪里，对于修补它们至关重要。通常，裂缝主要表现在软件编写存在bug、系统配置不当、口令失窃、明文通讯信息被监听以及初始设计存在缺陷等方面。一次次断网事件的发生，主要原因就在于漏洞的存在，让人有机可乘。 漏洞最常见就是软件编写过过程中存在的BUG，这是大多数软件系统都无法摆脱的，随着时间的推移总有一些意向不到得事发生，无论当初考虑的有多么周全。造成漏洞的还有系统配置问题，各部分功能重叠，或覆盖不够完整，或相互之间衔

接不够完美，都为非法行为提供了便利。对于这个问题，只有随时关注补丁的出厂时间，及时更新修补。同时，养成良好的习惯也至关重要。 漏洞的就相当于水，是使湖面不平静的内部条件。然而，一只巴掌拍不响，还需要外因，风险系数就是外部条件之一。无论做什么事我们都会考虑下值不值，就是经济学里投资回报率的问题，估计有的赚，风险小，才可以尝试。之所以一次次攻击服务器，是有人在这“ 投资 ”过程中得到了丰盛的回报，而且接近零风险。难怪会乐此不疲。对于这一状况，我们可以提高其难度，增加“ 投资 ”风险。倘若攻击一次服务器，就赔了夫人又折兵，谁还敢试？ 多次类似事件给网络安全行业乃至全社会敲了一次警钟。可以说，如今的互联网其实是很脆弱的，整个网络架构决定了，一旦DNS的服务器出现问题，后果会异常严重。互联网安全水平亟待提高。 编辑特别推荐: 如何改进存储利用率节约空间 网上冲浪怎样才能最high 如何实现DNS集中解析 关于域名抢注的那点事 解析和反向解析 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com