谈谈DNS安全问题——安全小课堂第三十期

2016-10-21 京东安全应急响应中心

安全小课堂第三十期

DNS就是把我们访问域名地址进行转换成对应IP地址的一种系统，DNS服务可以用于外部和公司内部，提供主机名到IP地址的转换。本期，我们来聊一聊DNS安全问题。

本期我们邀请到
唯品会安全专家Mils
猪八戒安全专家胡松林
大家欢呼
ヽ(*°▽°*)ﾉ

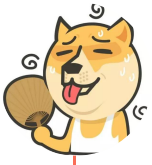
/ 01 /

豌豆妹

首先请科普下DNS吧。

小新 

DNS就是把我们访问域名地址进行转换成对应IP地址的一种系统，是Internet上作为域名和IP地址相互映射的一个分布式数据库。其实就是域名转换IP和IP转换域名的服务系统。

柴可夫斯基 

因为当用户在URL输入一个地址的时候，这些字母单词或者符号，计算机是无法理解

的，计算机只通过IP地址工作，所以DNS域名服务是将主机名解析成为IP地址的方法，当用户引用Internet上特定主机时候就可以采用主机名而非IP地址了。

/ 02 /

豌豆妹

那DNS服务的作用呢？

小新 

DNS服务可以用于外部和公司内部，提供主机名到IP地址的转换，类似于黄页提供人的姓名及他们相应的电话号码，我们更容易记住人的姓名和公司的名称，而不是电话号码或者IP地址。

小丸子 

DNS服务的作用就是，互联网上的主机都是用IP来进行标示的，如果大家上网都去记住IP是非常麻烦的，并不好记忆。为了能有更好的访问体验，和用户的记忆习惯，DNS就产生了，他主要负责把我们比较好记忆的域名转换成对应的主机IP。

/ 03 /

豌豆妹

能说说DNS面临的攻击么？

哆啦A梦 

DNS存在几个主要的安全隐患，容易遭受DNS欺骗（缓存感染、DNS信息劫持、DNS重

DNS存在几个主要的安全隐患，容易遭受DNS欺骗（缓存感染、DNS信息劫持、DNS重定向）、拒绝服务攻击、分布式拒绝服务攻击、缓冲区漏洞溢出等的攻击。

/ 04 /

豌豆妹

那从DNS安全角度考虑，如何防止那些攻击呢？

葫芦娃 

从网络的角度看，DNS控制与邮件控制类似，最安全的方法就是将内部网络DNS和外部网络隔开。
以下的控制手段可以加强在相应位置上对网络的控制，同时他们只可能在应用层工作，
这些限制方式包括：
不要将你的主从DNS服务器放在同一处进而隔离DNS服务器控制区域传输；
阻止想要获取你BIND版本的CHAOS查询进而隐藏BIND版本号；
及时更新系统补丁确保BIND等使用的是最新稳定版本；
关闭DNS服务器的glue fetching选项 option no-fetch-glue；
使用非root权限运行BIND /usr/local/sbin/named -u usera；
限定哪台主机能够发起区域传输和递归查询从而限制请求；
使用签名来认证区域传输；
使用高强度身份验证机制DNSSEC；
缩小系统DNS查询的重传次数和限制SYN频率从而提高系统响应能力；
控制你区域中的哪个部分对哪个子网可见。

小新 

另外还有8种最佳做法~可以结合网络拓扑看的那种~

（1）不要将你所有的DNS服务器放在同一区域。

通常在域环境中，最基本的DNS配置服务器有两台，一台服务器是域中的主服务器，另外一台则是从服务器。

当你的网络规模扩大时，你也许就会有多台主从服务器了，所以建议不要将你所有的DNS服务器放在同一区域，同时确保其连接至Internet出局链路路不同。因为如果你所有的DNS服务器全部连接到了同一条T1链路上，那一旦监听其他所有服务器上的缓存数据超时，只要该链路发起简单的flapping泛洪攻击就足以让你从Internet上消失，就是这种攻击在2001年1月重创了Microsoft公司，虽然Microsoft当年采用的链路比T1稍微大了那么点。

（2）拥有多台DNS主服务器。

如果你在域中只有一台DNS主服务器，那么即使你分散放置仍会遇到直接针对主服务器的Dos攻击，因为从服务器在SOA过期值定义的时间间隔内（通常是一个星期或更多）仍提供DNS数据，所以该攻击会持续更长时间；

（3）让你的外部DNS服务器仅响应非递归查询的请求。

DNS服务器能接收两类请求：递归查询与非递归查询。

（4）提供受保护的内部DNS服务器。

（5）分隔外部和内部DNS服务器提供的信息。

你往往有一些外部Internet用户不应该了解的内部系统，这些系统的DNS数据可以配置在你的内部服务器上，而不让他们出现在你的外部服务器上。

（6）限制主服务器的区域传输。

区域传输机制会将完整的域数据发送给请求数据的系统，而不是像通常那样只回答单个查询请求。

（7）用高强度身份验证机制DNSSEC。

DNSSEC使用了PKI和数字签名，这样DNS服务器可以验证消息的来源，从而确保他没有欺诈行为和潜在的恶意行为。

RFC 2535和3007对该技术进行了很好的概述。但在当前Internet基础设施中，还没有大量部署DNSSEC。

（8）HOSTS文件的保护。

DNS流量安全有一个问题是HOSTS文件的操纵，防止HOSTS文件的有效入侵方法，是将其设置为只读文件和实施主机型IDS，检测关键文件修改企图。

DNS其实内部有很多学问，刚才列举的内容还是不够齐全，前段时间自己正好也在用间隙时间看些资料，然后多实践下比较好。

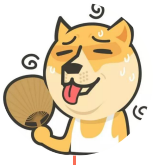
/ 05 /

豌豆妹

有时候我访问一些网站发现自己的网页会莫名奇妙的弹出一些广告或者是浏览网页发现

网络变慢，也是跟DNS有关么?

柴可夫斯基



对，这也有可能是DNS被劫持或做了转向。因为本机会首先去匹配HOST的缓存,然后在去DNS域名查询，可能在你之前访问网页时含有了一些恶意的脚本等代码修改了你本机的缓存。

豌豆妹

网站如何应对dns劫持呢？

哆啦A梦

应对DNS劫持，即使更换了自己的DNS地址还是没多大作用，因为出口还是会被运营商劫持，所以直接打电话投诉吧，感觉这招挺好使的。

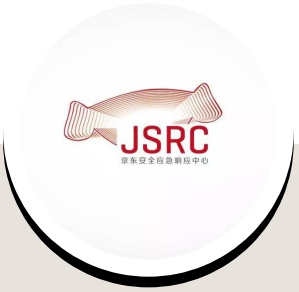
葫芦娃

DNS及时被劫持了，他也只会影响一个片区，除非DNS信息被扩散了。或者他本身就是劫持的顶级的DNS，或者你的提供商哒~

豌豆妹

好哒~棒棒哒~谢谢小伙伴们的耐心解答。咱们下期见哟！





微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂