ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.6,No.24, August 2010, pp.6687-6688,6706

E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

网络 DNS 欺骗攻击的检测及其防护

黎 成

(贺州学院,广西 贺州 542800)

摘要:DNS(Domain Name System)即域名服务系统,提供主机名字和 IP 地址信息的转换,它是联系整个网络的纽带,其安全的重要性不言而喻。而针对 DNS 服务器的欺骗攻击是攻击者常用的手法,但是目前的防范效果并不好。因此该文在前人研究的基础上,通过进行 DNS 欺骗攻击的实验,尝试在检测到欺骗之后发送正确数据包,试图找到一种简单而有效的防范策略,从而提高 DNS 的安全性和抗攻击性。

关键词:DNS;DNS 欺骗;DNS 数据包;攻击检测;防范

中图分类号:TP393 **文献标识码**:A **文章编号**:1009-3044(2010)24-6687-02

The DNS Deceive Detection and Prevention Technology Research

LI Cheng

(Hezhou University, Hezhou 542800, China)

Abstract: The DNS (Domain Name System) which provide host name and IP address convert, it is the whole network connection ligament, the importance of its safety is self-evident. And now for DNS server deceive against attack is commonly used gimmick, but the prevent effect is not good. So in this paper based on the former research, through the experiments of DNS deceive attack to detect deception, then sending correct packet, trying to find a kind of simple and effective prevention strategies, so as to improve the safety and aggressive of the DNS.

Key words: DNS; DNS cheat; DNS packet; attack detection; prevent

DNS 是大部分网络应用的基础,但是由于协议本身的设计缺陷,没有提供适当的信息保护和认证机制,使得 DNS 很容易受到攻击。一直以来,很多学者都在探讨 DNS 安全性的问题,对于 DNS 协议所固有的安全缺陷,给出了一些解决方案。IETF 的域名系统安全工作组提出了域名系统安全扩展协议 DNSSEC,该协议增加了认证机制,增强了协议本身的安全性。但是目前该协议在系统效率、密钥管理等方面还存在一定的问题,而且离大规模的普及和应用还有一定的距离。因此除了对 DNS 协议本身的安全研究之外,也有很多文章探讨了在现有的基础上的一些安全方案,主要是升级服务器软件,对 DNS 系统严格配置,禁止相关的功能等被动消极的防范手段,从整体上来说都是从增加 DNS 系统的可用性、可靠性、安全性方面着手的,此外还有一些可以躲避 DNS 欺骗攻击的可行性防范措施,比如:加权法、贝叶斯分类法等。

1 DNS 服务器工作原理

DNS 是一种实现域名名称与 IP 地址转换的系统,其工作原理是将域名到 IP 地址或将 IP 地址到域名的转换过程,也称为域名-地址解析。DNS 分为服务器端和客户端,服务器的公认端口号是 53。当客户端向服务器端发送映射请求时,本地 DNS 服务器首先会查询自己的数据库是否有对应的结果,若有则直接返回结果;否则要向上一级 DNS 服务器询问,以此类推直到获得结果,或者被告知查询结果失败,服务器必须做出回答。本地 DNS 服务器若获得结果将先保存在自己的高速缓存中,并回答客户端。

平常我们使用得最多的就是通过浏览器方式请求域名到 IP 地址的转换,即客户端向 DNS 服务器提交域名,请求对应的 IP 地址。现以所在校园网为例说明正常的 DNS 工作过程:假设现在有一台主机 IP 地址为 192.168.1.102,学校 DNS 服务器为 202.193.160.33,现在用这台主机访问谷歌网站,但是如果不知道其 IP 地址是多少,这时只能输入域名 www.google.cn 通过 DNS 查询其对应的 IP 地址。这个请求会从 192.168.1.102 的某个随机端口发送出去,由 202.193.160.33 的 53 号绑定端口接收并开始解析工作,这时先在 202.193.160.33 的缓存中查找 www.google.cn 的 IP 地址,如果存在就直接将其 IP 地址返回,若不在缓存中,则由 202.193.160.33 向外询问别的 DNS 服务器,然后把查询的结果先返回至 202.193.160.33,最后才由 202.193.160.33 将谷歌网的 IP 地址(203.208.39.99)返回给主机 192.168.1.102,这样 192.168.1.102 就可以和谷歌的站点建立连接并访问谷歌网站了,其具体过程如图 1。

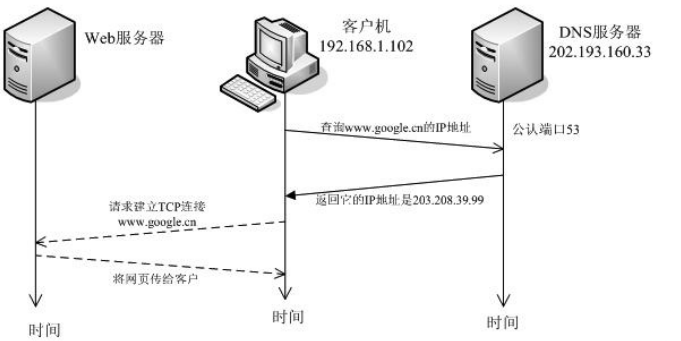

图 1 客户浏览器向 DNS 查询 web 服务器的 IP 地址[1]

2 DNS 欺骗原理

DNS 的查询请求和响应数据包是通过 DNS 报文的 ID 标识来匹配。在域名解析的整个过程中客户端首先以特定的 ID 标识向 DNS 服务器发送一个域名查询请求包,该标

收稿日期:2010-05-26

识是随机产生的。在 DNS 服务器查询出结果之后就会以相同的 ID 号给客户端发送响应包。在客户端收到响应包后,将其 ID 与原来发送的查询请求包的 ID 比较,如果匹配则表明接收到的正是自己等待的数据包,如果不匹配则抛弃。

针对 DNS 协议的特点,现在 Internet 上主要是抓住其协议的漏洞分别采取不同原理实施攻击:

1) 由于 DNS 报文只是简单的使用一个序列号来进行有效性鉴别,序列号由客户程序设置并由服务器返回结果,客户程序通过它来确定响应与查询是否匹配,这就引入了序列号攻击的危险;

2) 在 DNS 应答报文中可以附加信息,该信息与所请求的信息没有直接关系,因此攻击者就可以在应答中随意添加某些信息,指示某域的权威域名服务器的域名及 IP,导致在被攻击的域名服务器上查询该域的请求都会被转向攻击者所指定的域名服务器上去,从而对网络的完整性构成威胁;

3) DNS 的高速缓存机制,当一个域名服务器收到有关域名和 IP 的映射信息时,它会将该信息存放在高速缓存中,当再次遇到对此域名的查询请求时就直接使用缓存中的结果而无需重新查询。这样攻击者将 DNS 响应数据包的生存时间设置得很长,就能长期欺骗用户并不易被发现。

3 欺骗攻击方式

目前可行性的 DNS 欺骗的技术主要有内应攻击和序列号攻击两种方法。所谓内应攻击是指攻击者在非法或合法地控制一台 DNS 服务器后,直接操作域名数据库,修改指定域名所对应的 IP 为自己所控制的主机 IP 。当客户发出对指定域名的查询请求后,将得到伪造的 IP 地址。

序列号攻击则是指 DNS 协议格式中定义了序列号 ID 是用来匹配请求数据包和响应数据报, 客户端首先以特定的 ID 向 DNS 服务器发送域名查询数据包, 在 DNS 服务器查询之后以相同的 ID 号给客户端发送域名响应数据包。这时客户端会将收到的 DNS 响应数据包的 ID 和自己发送的查询数据包 ID 相比较,如果匹配则表明接收到的正是自己等待的数据包,如果不匹配则丢弃之。利用序列号进行 DNS 欺骗的关键是伪装 DNS 服务器向客户端发送 DNS 响应数据包, 并在 DNS 服务器发送的真实 DNS 响应数据报之前到达客户端,从而使客户端 DNS 缓存中查询域名所对应的 IP 就是攻击者伪造的 IP , 因此将客户端带到攻击者所希望的网站。

4 DNS 欺骗检测思路

根据序列号攻击方式的描述可知一个客户端在遭受 DNS 欺骗攻击的时候,至少会接收到两个序列号相同的应答包,其中一个是合法包,另一个则是欺骗包。根据这个特点就可以通过一些方法检测出这种攻击。目前可行的检测方法有以下两种:

1) 被动方式检测:该方式就是通过旁路监听的方式,捕获所有的 DNS 请求和应答数据包。正常情况下 DNS 服务器对一个查询请求包不会给出多个不同结果的应答包,即使目标域名对应多个 IP 地址,也只是有多个应答域,DNS 服务器会在同一个 DNS 应答包中返回。因此如果一段时间内,一个请求对应两个或两个以上结果不同的应答包,则怀疑其受到了 DNS 欺骗攻击。

2) 主动方式检测:所谓主动监测就是主动发送探测包去检测网络中是否存在欺骗攻击。在正常情况下发送这样的探测包不会收到任何应答,但是由于攻击者为了能在合法包之前将欺骗包送到客户端,所以不会对域名服务器 IP 的有效性进行验证,而是照样实施欺骗,由此收到应答包的就说明受到欺骗攻击了。

5 DNS 欺骗防范思路

在检测到存在 DNS 欺骗行为后,可以采取一些防范措施,比如:及时更新补丁或者使用代理就可以防范到 DNS 攻击。总的说来就只有两条:1) 直接用 IP 访问重要的服务,这样至少可以避开 DNS 欺骗攻击,但这需要你记住要访问的 IP 地址。2) 加密所有对外的数据流,对服务器来说就是尽量使用 SSH 之类的有加密支持的协议,对一般用户应该用 PGP 之类的软件加密所有发到网络上的数据。

本文针对序列号攻击,制作了一个客户端的我们只要捕获所有的 DNS 请求和应答数据包,如果较短的一段时间内,一个请求对应两个或两个以上结果不同的应答包,则提示其受到了 DNS 欺骗攻击,并将后到的那个合法包发送到 DNS 服务器将其 DNS 信息修改,这样在下次请求时就会得到正确的结果。

其检测和防范的流程图如图 2 所示。

6 DNS 欺骗攻击和检测防范系统实现

本系统使用 Visual Studio 2005.NET 中的 Visual C++语言来开发, 采用 winpcap 编程实施欺骗攻击和检测防范系统。

本系统通过连续抓取一段内的数据包,分析是请求包还是应答包,若是应答包则将其保存到一个数组中,否则不予理会。然后判断数组中的 DNS 数据报的 ID 是否相同,若这段时间内有相同的 ID 则说明检测出有 DNS 欺骗攻击,这时将取出后到的数据包再重发一遍,用正确的响应取代原来的欺骗包。DNS 欺骗检测防范的实现的部分代码如下所示:

```
if(udpr->sport == htons(53))//源端口为 53
{
 printf("收到应答数据包……\n");
 ……
if(dnsr1->id==dnsr2->id)
{
printf("注意! 你的机子已经受到 DNS 欺骗攻击! \n");//提醒有 DNS 欺骗,并发送一个正确的包过去
```

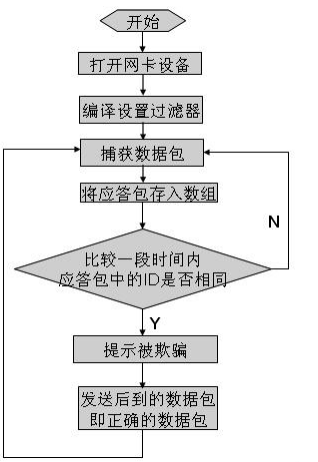

图 2 DNS 欺骗的检测和防范过程

(下转第 6706 页)

```
$graph->Add($pie);
$text=new Text("Types of Traffic",0,0)
$text->Pos(0.3,0.05);
$text->SetEont(FF_FONT1,FS_BOLD);
$graph->AddText($text);
$graph->Stroke();
```

安全响应模块:这个模块主要是实现收集入侵证据、调整网络环境和维护系统。安全响应是在系统遭到入侵后才会启动,因此安全相应启动前应该对入侵警报产生原因进行调查。实践过程中,作为网络维护的管理员,应该掌握准确可靠的信息,这样才可以提高入侵警报的处理效率和质量。

数据查询模块主要根据登录系统用户级别不同来同的查询范围和内容。如管理员可查询某时段击类型等主要入侵参数,并作相应的技术统计。

总之,校园网络安全问题给我们校园网管理者带来了极大的挑战,如果还只使用数据加密技术或者防火墙技术,这样无法达到对校园网络的安全保护。入侵检测系统能很好地弥补防火墙的不足,从某种意义上它是防火墙的补充,是整个安全防护体系的重要组成部分。入侵检测系统是一种主动防御的安全技术,它可以实现对内部攻击、外部攻击和误操作的有效的实时保护,因此受到学校网络安全的高度重视。

参考文献:

[1] 张颖,王辉.一种与入侵检测互动的 Internet 安全防范系统[J].计算机工程与应用 2003,(7).
[2] 石教英,蔡文立.科学计算可视化算法与系统[M].北京:科学出版社,1996.
[3] 吕良福,张加万,孙济洲等.网络安全可视化研究综述[J].计算机应用,2008,28(8):1924-1925
[4] ERICCOLE.黑客攻击透析与防范[M].北京:电子工业出版,2002.
[5] 戴英侠,连一峰,王航.系统安全与入侵检测[M].北京:清华大学出版社,2002.

(上接第 6688 页)

```
if (pcap_sendpacket(adhandle, savepack[pnum], sendcaplen /* size */) ! = 0)
{
    fprintf(stderr,"\nError sending the packet: \n", pcap_geterr(adhandle));
    return 0;
}
else  printf("Send DNS Spoof Packet Successfully! \n");
ischeat=true;
}
}
```

7 结束语

网络攻防一直是推动网络安全向前发展的动力,只有在不断的发现安全漏洞的同时不断改正,才能使整个网络更加健全和完善。本文所做的防范措施方面还是做得不够好,有时不能有效防范。这些只是阶段性的成果,要想真正做到完美,使 DNS 安全性真正让人放心,还需要在日后继续努力,做更深入的研究。

参考文献:

[1] 贺思德,申浩如.计算机网络安全与应用[M].北京:科学出版社,2007.
[2] (美)W. Richard Stevens.TCP/IP 详解,卷 1:协议[M].范建华,等,译.北京:机械工业出版社,2000.
[3] 滕步炜.DNS 欺骗技术的实现[N].连云港职业技术学院学报.2007(12),20(4).
[4] 姜春茂,黄春梅,聂福林.基于 DNS 攻击的安全防范策略[J].陕西科技大学学报,2004(12):150-500.
[5] 闫伯儒,方滨兴,李斌,王箦.DNS 欺骗攻击的检测和防范[J].计算机工程,2006,32(21).
[6] 陈鸿星,张红霞,林淑琴. RFC 特征剖析及网络安全性对策[J].实验室研究与探索,2008,27(11).