ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.12, No.11, April 2016
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

典型网络欺骗攻击原理及防范的研究

罗玉梅

（贵州师范大学，贵州 贵阳 550001）

摘要：随着计算机网络的飞速发展，网络承载的业务数量及种类越来越复杂，安全问题也不断出现。其中，网络攻击问题尤为严重，不仅妨碍网络用户的正常使用，更严重的甚至会影响到整个网络的正常运行。该文分析了几种主要攻击的实现过程及特征，从而提出相应的防御措施。

关键词：ARP欺骗攻击；DNS欺骗攻击；IP欺骗攻击；防御攻击

中图分类号：TP393 文献标识码：A 文章编号：1009-3044(2016)11-0036-02

DOI:10.14004/j.cnki.ckt.2016.1260

1 引言

伴随着网络应用的不断发展，网络安全问题层出不穷。正是由网络本身具有的开放性、互联性、多样性以及不均匀性等特征，使其极易受到各种攻击；因此，如何保障网络的安全是当前面临的首要问题。

网络欺骗攻击就是利用网络存在的安全缺陷进行攻击。在实施攻击的过程中，攻击方会极力想办法得到网络的信任，其原因是网络操作都是倾向于可信系统[1]。一旦建立乐信任关系，受信系统的管理员就能够实施工作并维护相应的系统安全级别。通常，如果一个系统A是受到另一个系统B的信任的，此时若有一个系统C假装成B，则C就轻易地获得B的一些权力。

2 几种主要的网络欺骗攻击

2.1 ARP欺骗攻击

ARP协议的主要功能是将IP地址转换成对应的MAC地址，依靠在内存中保存的转换表让IP能够在网络中获得目标主机的响应。在ARP协议中，为了减少数据的通信的数据量，主机会将收到的ARP应答包插入到自己的ARP缓存表中，不论这个包是否是自己所请求的，如此便使ARP欺骗实施成为可能[2]。如图1所示，若攻击者想获知网络中两个用户间的通信，向两个用户主机发送一个ARP应答包，此时两个用户都会将攻击者的主机MAC地址误以为是对方的MAC地址。如此一来，攻击者便可以获知双方通信的内容，通信双方看似直接通信的过程，中间实际都是通过攻击者的主机来间接实施的[3]。

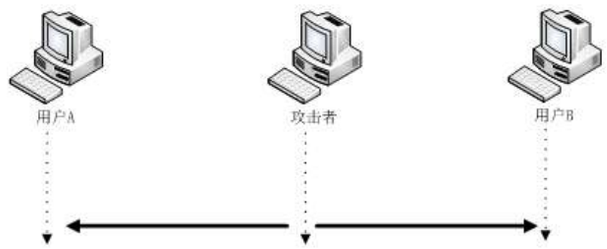


图1 ARP欺骗过程示意图

2.2 DNS欺骗攻击

域名系统（DNS）是一种分布式数据库，主要用于实现主机名和IP地址的转换，是广大网络应用的基础。然而协议本身存在的设计缺陷且没有适当的信息保护和认证机制，导致DNS极易受到攻击[4]。在DNS解析过程中，客户端先向DNS服务器发送查询数据包，随后服务器将查询结果用相同的ID号发回给客户端。客户端将响应数据包的ID与之前发送的查询包的ID进行比较，若一致，则说明此响应数据包正是自己的。在此过程中，若攻击者假冒DNS服务器提前给客户端发送响应数据包，客户端收到的域名对应的IP地址就可由攻击者指定了，当客户端访问所需网站时实际上访问到的是攻击者指定的网站[5]。攻击过程如图2所示。

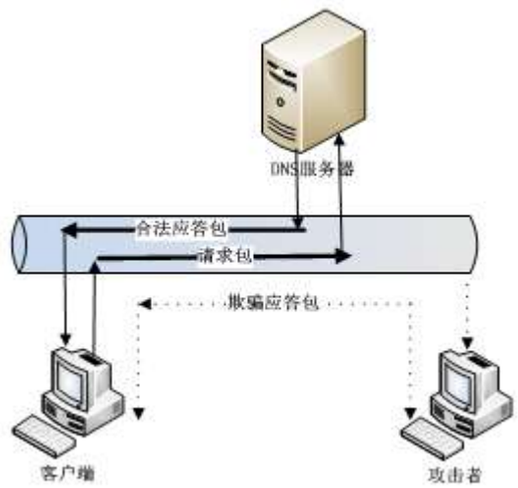


图2 DNS欺骗攻击

2.3 IP欺骗攻击

IP欺骗是一种伪造数据包源IP地址的攻击，即是向目标主机发送源地址非本机IP地址的数据包。攻击的简要过程如图3所示，攻击方X对目标B实施拒绝服务攻击使其崩溃无法应答，随后向A发送源地址为B的数据包，尝试与A建立连接，从

收稿日期：2016-03-24

而达到欺骗的目的。

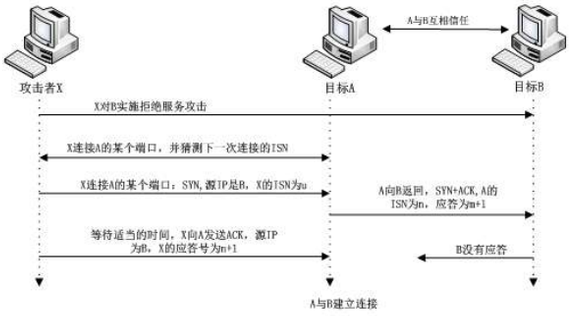


图3　IP欺骗简要过程

3 网络欺骗攻击的防御

3.1 ARP欺骗攻击的防御及测试

在ARP欺骗攻击过程中需同时欺骗网络中的其他主机和网关交换机，从而实施“中间人攻击”。可以从以下方面进行控制：

（1）将网管的ARP表项绑定到用户的主机上，防止中间攻击者的arp relay报文更新用户的网管ARP表。

（2）将用户主机的ARP表绑定到网关交换机，防止中间攻击者的arp relay报文更新网关交换机的ARP表。

防御ARP攻击的方法很多，例如：

（1）在交换机上阻止“中间人攻击”。通常，在支持网管的交换机上都能绑定用户的 ARP，通过端口的 port security 将端口上的可学习 MAC 数及用户主机的 MAC 地址进行绑定，或使用 dhcp snooping 将用户主机的 IP 地址和 MAC 地址进行绑定。

（2）在用户主机上控制“中间人攻击”。 在接入交换机上启用 pvlan 或者 port-isolated 功能隔离不同用户，从而使被攻击主机的 arp relay 不能发给网络上其他主机。

（3）在端口开启 802.1x 认证，利用 802.1x 客户端实现二层网络的用户认证，将帐号、端口及 MAC 等信息和用户终端绑定，从而防止中毒的主机侵入内部网络。

实验测试环境如图4，在网络中用户主机上不能ping通公网地址，有的主机甚至ping不通自己的网关。

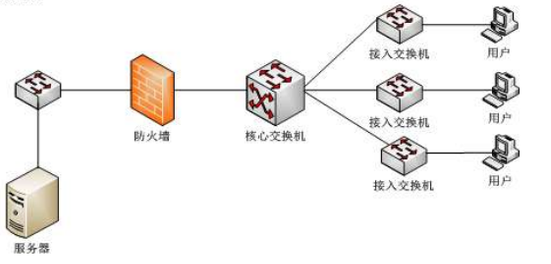
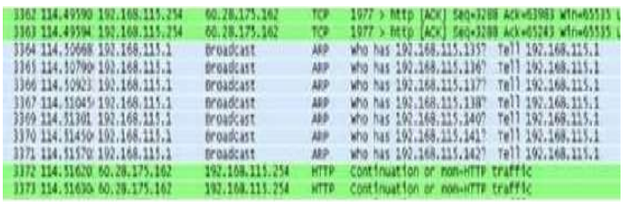


图4　实验拓补图

在核心交换机上抓取的数据包如下：



从故障的表现及抓包的情况可以判定是受到ARP攻击；随后，将连接发送大量ARP数据包主机的交换机断电，网络上其他用户能够正常上网。为了防止再次受到类似攻击，可以采取如下措施：

1）在每个接入交换机上进行MAC绑定，对端口的接入主机数进行设定。

2）在核心交换机上实施IP与MAC绑定，阻止虚假arp数据进入网络；同时，开启抑制广播风暴功能，防止核心交换机因内存或CPU占用过高影响接入交换机工作。

3）在防火墙上布置安全策略。

4）在有访问权限的主机上做一个批处理，将本机 IP 与MAC进行绑定，同时将本机网关的IP与MAC绑定。设置开机启动该批处理程序。

3.2 DNS欺骗攻击的防御

DNS欺骗攻击的实现主要包括中间人攻击和缓存投毒攻击两种形式，其中中间人攻击主要针对的对象是DNS查询客户端。防御DNS欺骗攻击，必须要同时保护DNS客户端和DNS服务器。由此，给出防御DNS欺骗的解决方法如下：

（1）对于网络中有设定的DNS服务器，要及时更新服务器的版本，将动态更新和区域传输范围进行限制。

（2）对用户主机来说，防御DNS的主要措施有如下几点：1）禁用主机DNS缓存；2）给主机指定DNS服务器和本地UDP端口号。通过指定UDP端口号，防火墙的设置更加精确，从而能够进一步提高整体安全性。

3.3 IP欺骗攻击的防御

IP欺骗攻击的原理比较简单，但实际实施却很困难，需要进行序列号猜测和建立信任关系等过程。然而要成功实施IP欺骗也不无可能，因此，也要对IP欺骗攻击进行防范，主要方法有：

1）尽量不要使用源地址认证的服务系统以及基于IP的认证机制，对于远程Telnet服务考虑由SSH替代。

2）在边界路由器上采取源地址过滤措施，检查进入本网数据包的源IP，防止使用本地IP的外部数据进入本网络，从而防御IP欺骗攻击。

4 总结

对网络来说，除了满足功能性需求外，还要保证网络的安全，防止网络受到各种安全性攻击。在网络安全中协议漏洞是最严重的安全漏洞，给攻击者创造了成功机会。ARP欺骗攻击正是利用了 ARP 协议自身的安全漏洞，通过专用攻击工具让攻击极易成功。IP欺骗攻击也是利用TCP/IP协议存在的漏洞来实施的。对于类似网络攻击，用户除了做好网络和终端设备等硬件的安全防范工作外，还要不断提高安全意识，不断了解防范欺骗类攻击的最新技术，真正做到防患于未然。

参考文献：

[1] 谢希仁.计算机网络(第五版)[M].北京:电子工业出版社,2008.
[2] 李浩.ARP.病毒攻击分析及其防御措施[J].宁波广播电视大学学报,2007.
[3] 李成友,韩昧华.互联网协议中地址解析的欺骗问题研究[J].网络安全技术与应用,2010.
[4] 郑亚,谢琳.DNS的原理及其应用[J].软件导刊,2012.
[5] Hudaib Z. DNS Advanced Attacks and Analysis[J]. International Journal of Computer Science and Security (IJCSS),2014.