ARP 欺骗原理及保护方法

学号:XXXXXXX 姓名:追逐繁星的苍岚
北京理工大学计算机学院 x 班，北京 100081

Principle of ARP Spoofing and Protecting Method

Student ID: xxxxxxx Name: ZHUIZHUFANXINGDECANGLAN
Class X,School of Computer Science, Beijing Institute of Technology, Beijing 100081

Abstract: ARP spoofing is an attack method in which the attacker responds to ARP requests from legitimate clients by broadcasting illegal ARP responses, thereby impersonating communication devices on the LAN. Therefore, legitimate clients may forward traffic to unintended communication partners, leading to information eavesdropping. This report will explain the attack principles, specific applications, history and development of ARP spoofing, and preventive countermeasures from various aspects.

Key words: ARP spoofing; kali

摘要: ARP 欺骗是一种攻击方法，攻击者通过广播非法 ARP 响应来响应来自合法客户端的 ARP 请求，从而冒充局域网上的通信设备。因此，合法客户端可能会将流量转发给非预期的通信伙伴，从而导致信息窃听。本次报告将从多方面阐述 ARP 欺骗的攻击原理、具体应用、ARP 欺骗的历史与发展以及预防对策等。

关键词: ARP 欺骗；kali

我们生活在信息大爆炸的年代，由于信息科技的不断发展，我们通过互联网获取的知识和情报越来越多，无线连接设备的数量在不断增加并渗透到社会的各个领域当中。随着这些信息交互手段的进步，专门针对互联网交互的恶意第三方网络攻击也成为一个需要解决的问题。在基于这样的背景情况下，本次报告我将重点讨论来自无线终端的网络攻击 ARP 欺骗。ARP 欺骗又被称之为 ARP 毒化或 ARP 病毒，这是一种专门针对以太网地址解析协议的渗透攻击技术，它的工作原理十分简单，首先假设有一位诚实合法的客户端发送 ARP 请求以将数据包转发到默认网关的路由器，网关发送自己的 ARP 响应和 IP 地址、MAC 地址等，这时候在同一局域网下的恶意攻击者将通过局域网广播不断发送伪装后的非法 ARP 响应，合法客户端在收到这些无效的 ARP 响应后，会将发送这些的攻击者的 MAC 地址更新在自己的 ARP 表中，从而导致在下一次的数据传输当中会将数据包转发给恶意攻击者，使合法客户端的流量被恶意攻击者窃听到。攻击恶意者也可以将这些数据包篡改后再发送给合法客户端，从而混淆数据的正确性，达到恶意破坏的效果。

1. ARP 欺骗的具体应用

1.1 ARP 欺骗的五种常用攻击手段介绍

如上文所述，ARP 欺骗攻击最经常使用的攻击手段之一便是制造一个中间人攻击，在两个合法的客户端之间进行数据的破坏或是篡改、监听等动作。在基于这种中间人攻击的情况下，如果没有专门的防火墙保护，诚实的合法用户很难去辨别自己是否受到了 ARP 攻击。但是除了中间人攻击以外，还有另外四种攻击也是被经常广泛使用的。本次实验我将复现出这五种 ARP 欺骗的攻击方式，并阐释其中的攻击原理。从实践中了解关于 ARP 欺骗的一些基本知识以及具体的应用。

ARP 欺骗的五种攻击手段当中，第一种攻击手段是针对路由器 ARP 表的欺骗，[1]针对路由器 ARP 表

的欺骗原理是截获相对应的网关数据包，ARP 欺骗会在同一局域网下通过广播不断发送虚假的 ARP 响应，然后通知路由器错误的 MAC 地址，并按照一定频率去刷新，使真实的地址无法更新在路由器的 ARP 表当中，这样做的结果就是路由器的所有数据都只能发送给恶意攻击者的 MAC 地址，使合法客户端无法收到信息，从而造成重大损失。

第二种攻击手段则是针对内网 PC 的网关欺骗。针对内网 PC 网关欺骗的原理是伪造网关，ARP 欺骗首先先制造一个虚假的网关，然后让被欺骗的合法客户端的主机向这个虚假网关发送数据，而并非通过正常路由器网关上网，这么做的结果就是合法客户端的主机将无法连上网络，从而造成持续掉线状态。

第三种攻击手段则是在第二种攻击手段的基础上限制网速，由于合法客户端此时的网关被攻击机冒充，因此当要访问网络时就不得不经过恶意攻击者冒充的网关，这时恶意攻击者只要限制自己的网关流量速度就可以达成对合法客户端的限速效果了。

第四种攻击手段则是通过获取到的数据流量来达成嗅探数据的目的。在 ARP 欺骗当中不仅可以嗅探到加密的数据包，还可以获取合法客户端访问的图片、网页、账号密码等资料。

最后一种攻击手段则是 DNS 欺骗。这是一种结合 ARP 欺骗的攻击手段。将合法客户端要访问的网页强行指向另一个域名，也就是重定向域名的 IP 地址，通常这个重定向的 IP 地址都是恶意攻击者控制的。利用这种技术，恶意攻击者可以很轻松的伪造一个虚假的钓鱼网站或是在某个网站后台挂马，在合法客户端访问的那一瞬间自动下载后台的木马病毒到主机，从而使合法客户端的主机中木马病毒。DNS 欺骗也是最难判断的攻击手段之一。举个例子：当合法客户端访问 www.baidu.com 这个网址的时候，由于受到 DNS 欺骗攻击，网站在访问的一瞬间被重定向到由恶意攻击者冒充的虚假网站 www.baldu.com，而且这个网站的前端界面设计和百度官网一模一样，合法客户端根本不会认为自己此时已经被受到 DNS 欺骗攻击，而在这个网页下填写的百度账号和密码都将被嗅探到，达到盗取账号的目的。

需要强调的是，以 ARP 欺骗为攻击原理的木马病毒具有很强的传染性，一旦被这种木马病毒感染一台主机就很有可能导致整个局域网都陷入到 ARP 欺骗攻击当中，使整个局域网内的主机都无法上网，从而导致网络瘫痪的效果。

1.2 针对 Windows7 的 ARP 欺骗—基本应用测试

[2]在本次渗透测试中我将使用 kali linux 系统作为渗透攻击测试平台，Windows7 系统作为实验靶机。

kali linux 主机的 IP 地址为：

192.168.8.147

Windows7 主机的 IP 地址为：

192.168.8.148

首先利用 nmap 扫描当前局域网下的所有主机 IP 地址，在得到所有主机地址后可以发现实验靶机的 IP 地址如图 1，通过 ifconfig 指令可以看到我们的内网 IP 地址是 192.168.8.255，因此可以得知实验靶机的内网也是 192.168.8.255，可以看到靶机的 Host 是开启状态的。

这个时候就可以进行 ARP 欺骗攻击了，由于 kali 自带 arpspoof 工具，因此可以直接输入攻击指令：

arpspoof -i eth0 -t 目标靶机的 ip 主机的 ip；

这里的主机变成了路由器，通过 fping 指令可以很容易查看到主机的 IP 地址，攻击机的攻击效果如图 2 所示，靶机的结果如图 3 所示。

```
└─# nmap -sP 192.168.8.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 19:20 CST
Nmap scan report for 192.168.8.1
Host is up (0.00054s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.8.2
Host is up (0.00037s latency).
MAC Address: 00:50:56:EB:F9:65 (VMware)
Nmap scan report for 192.168.8.148
Host is up (0.00058s latency).
```

图 1 扫描局域网得到的所有主机 IP 地址

```
┌──(root㉿kali)-[/home/linuxcc/桌面]
└─# arpspoof -i eth0 -t 192.168.8.148 192.168.8.2
0:c:29:a5:cb:45 0:c:29:cf:b7:85 0806 42: arp reply 192.168.8.2 is-at 0:c:29:a5:cb:45
0:c:29:a5:cb:45 0:c:29:cf:b7:85 0806 42: arp reply 192.168.8.2 is-at 0:c:29:a5:cb:45
0:c:29:a5:cb:45 0:c:29:cf:b7:85 0806 42: arp reply 192.168.8.2 is-at 0:c:29:a5:cb:45
```

图 2 kali 攻击机下运行 ARP 欺骗的攻击截图

图 3 受到 ARP 欺骗攻击的 win7 靶机无法上网

在进行攻击前，在 win7 靶机上输入 arp -a 指令后可以显示当前主机更新缓存的 IP 地址和 MAC 地址对应表如图 4 所示，由于主机 IP 充当了路由器，因此可以看到当前网关的 MAC 地址为：

00-50-56-eb-f9-65；

192.168.8.147 是攻击机的 IP 地址，可以看到攻击机对应的 MAC 地址为：

00-0c-29-a5-cb-45；

在进行攻击的时候，重新输入指令，可以看到结果如图 5，主机的 MAC 地址变成了和攻击机一模一样。由于返回的 MAC 地址是攻击机的，因此靶机无法上网。

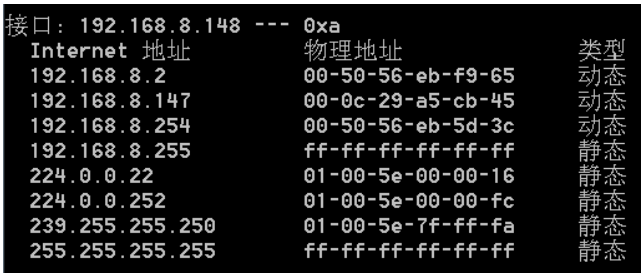

图 4 win7 靶机被攻击前的当前网关的 MAC 地址

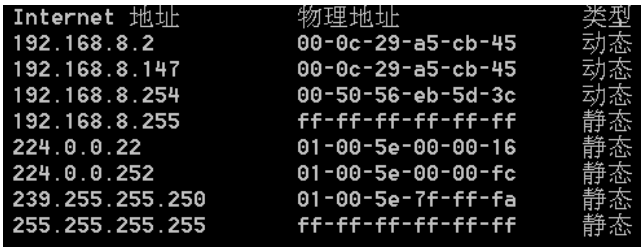

图 5 win7 靶机被攻击时的当前网关的 MAC 地址

1.3 Windows7 下 ARP 欺骗--流量转发与监控

[3]本次实验的目的是为了利用 ARP 欺骗攻击来完成对于 win7 实验靶机的流量转发与监控，并将捕获到的流量进行分析。首先先在桌面上新建一个 txt 文件，在里面写入自己的 IP 地址和*.*.*，如下图 6 所示。

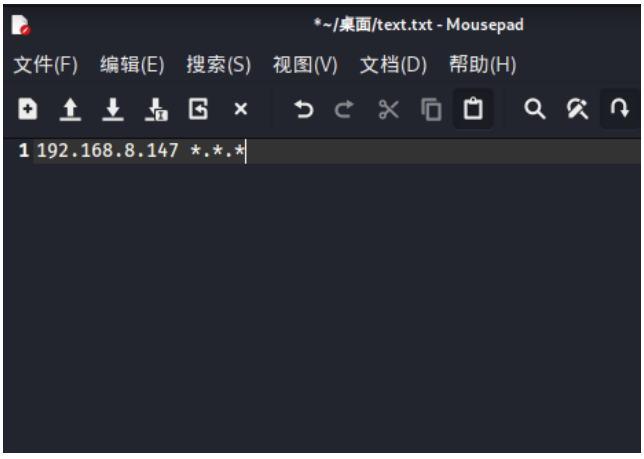

图 6 TXT 文本内容

在 kali linux 终端上输入以下命令：

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

上面命令的功能是配置 linux 系统的 IP 转发功能，同时输入命令：

cat /proc/sys/net/ipv4/ip_forward；

这一段命令的功能是查看流量转发的状态。

之后的步骤和 1.2 相同，在将靶机的网关 MAC 地址修改成攻击机的 MAC 地址后，输入指令如图 7，得到实验靶机正在请求的数据资料如图 8，左边是 Windows7 虚拟机的预览器显示的图片，右边则是攻击机监控到的图片。实现了监控实验靶机数据流量的目的。

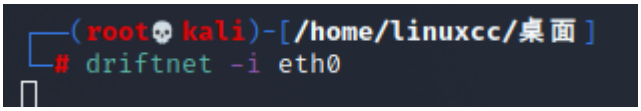

图 7 打开流量监控指令

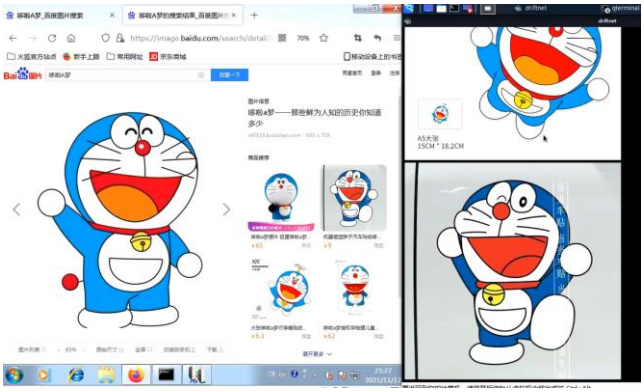

图 8 获取到的 win7 实验靶机数据流量图片

1.4 Windows7 下 ARP 欺骗--限制网速

ARP 欺骗还可以限制实验靶机的网络速度。在实验 1.3 将靶机毒化后，此时靶机所使用的网关是攻击机伪造的虚假网关，攻击机可以通过下面这一条指令来限制对于靶机的网络速度：

sudo tc qdisc add dev eth0 root netem delay 时间;

可以看到结果如图 9，利用 ping 指令向对方传送数据包后传达回来的时间基本都在 200ms（通过上一条指令将网速限制在 200ms）。值得注意的是，在限制靶机的网速之前一定要开启路由转发功能，否则就无法实现限速的效果。

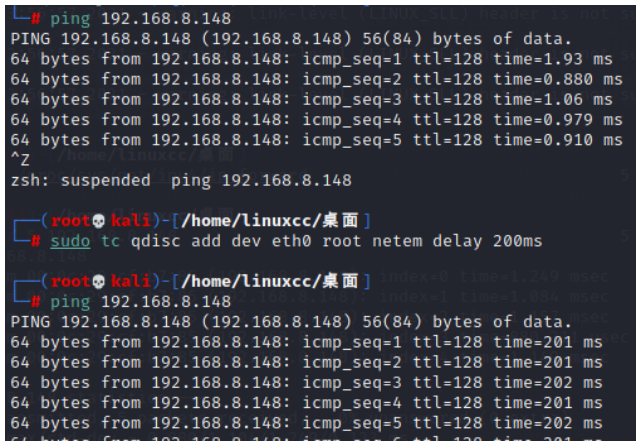

图 9　限速前后的 ping 对比， ping 后时间都在 200ms 左右

1.5 Windows7 下 ARP 欺骗—盗取账号密码

由于在实验 1.4 中开启了路由转发功能，所以本次实验就不用再开启了，否则一定要开启后才能实现嗅探数据功能。在毒化实验靶机后，打开 wireshark 工具来进行数据分析，可以看到大量加密数据包如图 10。由于本次实验的目的是为了实现关于密码账号的嗅探，因此要使用 dsniff 这款工具。重新打开一个新的终端，在终端下输入如下指令：dsniff -i eth0 -m;这时 dsniff 开始截获账号密码，结果如图 11 所示，可以看到合法客户端登陆了账号 helloworld，密码是 123456。

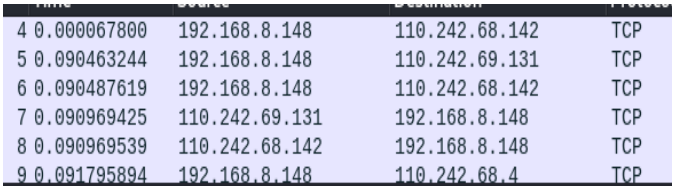

图 10　利用 wireshark 捕获到的加密数据包

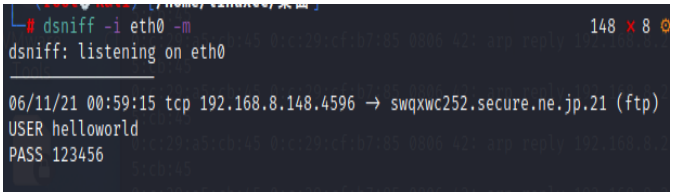

图 11　利用 dsniff 嗅探得出来的账号密码

1.6 Windows7 下 ARP 欺骗和 DNS 欺骗

DNS 欺骗将合法客户端要访问的某网站的域名重定向为另一个域名，通常这个域名是恶意攻击者自己搭建的网站。利用 dnsspoof 工具，如果 dnsspoof 嗅探到局域网内有关于 dns 的请求数据包，就会伪造虚假的 dns 响应来回复请求的对象。dns 查询需要合法客户端像网关发起请求，因此还是要配合 ARP 欺骗攻击来使用。

通过上面步骤的实验完成了攻击机对于合法客户端网关的假冒后，更新 locate 数据库，查找 locate 命令定位的文件的位置，然后利用 vim 工具修改文件的信息，在最后一行加入 IP 地址和对应的网址，本次实验所采用的网站是百度官网 www.baidu.com，跳转到的网页是攻击机的 apache 网址，输入以下命令：

dnsspoof -i eth0 -f 文件路径/dnsspoof.hosts;

可以看到结果如图 12，当合法客户端访问百度时，自动跳转到了 apache 网址。

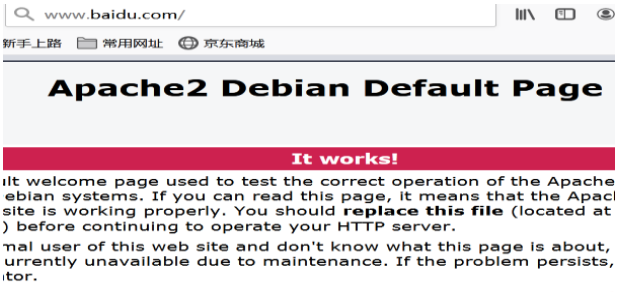

图 12　跳转到 apache 网址

2. ARP 欺骗的历史事件与发展

2.1 ARP 病毒的历史事件

由于 ARP 协议在最开始设计的时候并没有为其设计相关的安全协议，这就导致了 ARP 协议可以接收到局域网内的任意 ARP 协议包，从而为 ARP 欺骗提供了恶意行为的可能性。**[4]**将这种技术与病毒技术相结合产生出来的 ARP 欺骗病毒属于木马病毒类型，但是却不具有自我复制与传播的功能，当病毒开始工作时会向因特网发送虚假伪造的 ARP 数据包，以此来干扰网络的工作效率。

ARP 病毒早在 2010 年以前就十分盛行，那时候流行的热门网页游戏当中就出现了专门针对数据包传输破坏的 ARP 病毒。主要表现为通信之间的缓慢和断网等功能，一旦某局域网下的一台主机中了 ARP 病毒的话就会影响到该局域网下的所有主机，因此这种类型的 ARP 病毒在当时对于局域网的影响甚至比黑客盗取游戏账号等所造成的破坏还要大上许多。

2.2 ARP 病毒的发展

自那之后 ARP 病毒便开始迅速发展，到后来甚至可以通过对于网络电话的劫持来达到在计算机上网的时候插入特定恶意代码的效果，同时利用 DNS 欺骗相结合来达成计算机在访问其他网站时强制跳转到另外一个网站上面并下载网站里的木马、病毒等，同时还可以嗅探到合法用户在计算机上登录的账号和密码的数据信息，给合法用户造成极大的损失。

同时，随着互联网科技进步的发展，越来越多基于 ARP 欺骗攻击原理的渗透工具也逐渐被大众所知，ARP 欺骗攻击已经不再是专业的黑客才能掌握的技术，针对它的预防对策也越来越多，图 13 为目前被许多计算机爱好者广为流传使用的基于 ARP 欺骗原理的嗅探工具 ettercap。因此，知晓这类恶意攻击的检测方法与预防对策是非常有必要的一件事情。

图 13 ettercap 是一款基于 ARP 欺骗的嗅探工具

3. ARP 欺骗的检测与预防对策

提高用户的安全意识是抵御欺骗攻击的最重要对策。本节将阐述针对 ARP 欺骗的检测方法与预防对策，具体的方法如下：

3.1 终端输入命令检测

[5]打开主机的 cmd 命令终端，输入指令：arp -a 来查看计算机的 ARP 缓存表状态，如果发现 ARP 缓存表当中有网关信息之外的记录且网关的 MAC 地址和网关之外的 IP 地址的 MAC 地址一样的话，就说明本台主机可能受到了 ARP 欺骗攻击。

3.2 缓存超时检测

计算机在一般情况下只有发送了 ARP 请求后才会收到响应，且 ARP 缓存表要过一段时间才会失效。但是对于恶意攻击者来说，为了保证长时间截获合法客户端计算机的数据信息，就必须维持对该计算机的 ARP 缓存欺骗，且这个时间限制必须要小于合法计算机的缓存表项超时时限。所以诺是在合法计算机的缓存表项超时时间内收到的应答包不止一个的话，就可可能受到了 ARP 欺骗。

3.3 通过安装防火墙来预防攻击

通过安装 ARP 防火墙，可以保护计算免受来自外部的未经授权的访问，但是在 ARP 欺骗攻击中，通过将 IP 地址伪装成私有地址，很可能会使攻击通过防火墙。因此，如果使用内部私有地址进行外部访问的话可以通过设置不允许通信来保护计算机免受 ARP 欺骗攻击。

3.4 通过设置静态的 ARP 缓存来预防攻击

通过在计算机上添加静态的 ARP 缓存记录。如果恶意攻击者向主机发送 ARP 响应报文，合法计算机接收到后不会更新 ARP 缓存表。从而避免 ARP 欺骗的攻击。但是这种方法也有着不少缺点，比如需要合法用户手动设定静态 ARP 缓存，如果计算机自动获取到新的 IP 地址或更换新的网卡后，合法用户就必须重新手动设置；另外就是恶意攻击者可以对 ARP 病毒进行重新编码来使病毒具有破坏 IP-MAC 绑定的功能，使合法用户设置的 ARP 缓存无效。

4 结束语

本文介绍了 ARP 欺骗攻击原理与攻击类型、发展历史和预防对策这三个模块。ARP 协议在最初由于效率问题并没有为其设计安全协议，因此它的安全性能相当脆弱。ARP 欺骗最常见的攻击方式是泛洪攻击、流量监控、网关欺骗、嗅探数据和 DNS 欺骗等，其中嗅探数据和 DNS 欺骗造成的损失最多。ARP 欺骗在初期主要被利用与木马病毒上，通过木马病毒来达到阻碍某一局域网下所有主机的通信以及嗅探主机的信息，盗取用户的账号密码等功能。针对 ARP 欺骗的检测中，最常用的两种方法是检查 ARP 缓存表和超时缓存检测，可以通过安装 ARP 防火墙或是设置静态 ARP 缓存来达到预防 ARP 欺骗攻击的效果。

参 考 文 献

[1] nextgreen. [Z]. CHINA: Arp 欺骗有几种类型, 2007

[2]橙子 youTA. [EB/OL]. CHINA: kali linux 进行 arp 欺骗, 2018

[3] sss-lql. [EB/OL]. CHINA: kali 冒充路由器开启 ARP 局域网欺骗, 2020

[4] 刘卫华. [M]. CHINA:ARP 欺骗攻击研究及 ARP 安全防护的实现, 2009

[5] whoim_i. [EB/OL]. CHINA: arp 欺骗攻击与防范技术总结和分析, 2020

[6] 松藤央 落合秀也 江崎浩. [M]. JAPAN: 無線端末による ARP を用いた セグメント内の通信妨害攻撃とその対策, 2018

[7] d0main. [EB/OL]. CHINA: ARP 工作过程、ARP 欺骗的原理和现象、如何防范 ARP 欺骗, 2017

[8] 神薗 雅紀. [Z]. J APAN: 公衆無線 LAN への攻撃手法, 2017