使用 ARP 分组检测处于混杂模式的网络节点

1.简介

在局域网中，嗅探行为已经成为网络安全的一个巨大威胁。通过网络嗅探，一些恶意用户能够很容易地窃取到绝密的文档和任何人的隐私。要实现上述目的非常容易，恶意用户只要从网络上下载嗅探器并安全到自己的计算机就可以了。然而，却没有一个很好的方法来检测网络上的嗅探器程序。本文将讨论使用地址解析协议(Address Resolution Protocol)报文来有效地检测办公网络和校园网上的嗅探器程序。

2.网络嗅探的原理

局域网通常使用以太网进行连接。在以太网线缆上使用 IP(IPV4)协议传输的传递的信息是明文传输的，除非使用了加密程序进行了加密。当一个人把信息发送到网络上，他会希望只有特定的用户才能收到这些信息。但是，非常不幸，以太网的工作机制为非验证用户提供了窃取这些数据的机会。以太网在进行信息传输时，会把分组送到各个网络节点，目的地址匹配的节点会接收这些分组，其它的网络节点只做简单的丢弃操作。而接收还是丢弃这些分组由以太网卡控制。在接收分组时，网卡会过滤出目的地址是自己的分组接收，而不是照单全收。在本文以后的部分我们将把网卡的这种过滤称为硬件过滤(Hardware Filter)。但是这只是在正常情况下，嗅探器使用另一种工作方式，它把自己的网卡设置为接收所有的网络分组，而不管分组的目的地址是否是自己。这种网卡模式叫作混杂模式(Promiscuous Mode)。

3.检测混杂模式的基本概念

在网络中，嗅探器接收所有的分组，而不发送任何非法分组。它不会妨碍网络数据的流动，因此很难对其进行检测。不过，处于混杂模式(promiscuous mode)网卡的状态很显然和处于普通模式下不同。在混杂模式下，应该被硬件过滤掉的分组文会进入到系统的内核。是否回应这种分组完全依赖与内核。

下面我们举一个现实世界中的例子，说明我们检测处于混杂模式网络节点的方法。设想一下，在一个会议室中正在举行一个会议。某个人把耳朵放在会议室就可以进行窃听(嗅探^_^)。当她(还是个女的，原文如此:P)进行窃听(嗅探)时，会屏住呼吸，安静地聆听会议室内所有的发言。然而，如果此时会议室内有人忽然叫窃听者的名字：“XX 太太”，她就可能答应“唉”。这听起来有点好笑，但是完全可以用于网络嗅探行为的检测。网络进行网络嗅探的节点会接收网络的所有报文，因此其内核可能对某些本该被硬件过滤的分组作出错误回应。根据这个原理，我们可以通过检查节点对 ARP 报文的响应来检测网络的嗅探行为。

4.基础

1).硬件过滤器

首先，我们从处于混杂模式(promiscuous mode)下和普通模式下有何不同开始。以太网的地址是 6 个字节，制造商为每块网卡分配的地址在全世界是唯一的，因此理论上没有相同地址的网卡。在以太网上的所有通讯都是基于这种硬件地址。

不过，网卡可以被设置为不同的过滤模式以接收不同种类的分组。下面就是以太网卡的过滤模式：

unicast

网卡接收所有目的地址是自己的分组

broadcast

接收所有广播分组，以太网广播分组的目的地址是 FFFFFFFFFFFF。这种广播分组能够到达网络上的所有节点。

multicast

接收目的地址为指定多投点递交(multicast)组地址的分组。网卡只接收其地址已经预先在多投点列表中注册的分组。

all multicast

接收所有多投点递交广播分组。

promiscuous

根本不检查目的地址，接收网络上所有的分组。

图-1 描述了硬件过滤器处于在正常情况下和在混杂模式下的区别。通常，网卡的硬件过滤器被设置为接收目为单投点递交(unicast)、广播(broadcast)和多投点递交(multicast)地址 1 的分组。过滤器只接收目的地址为自己的地址、广播地址(FF FF FF FF FF FF)和多投点地址 1(01 00 5E 00 00 01)的分组。

2).ARP 机制

使用以太网连接的 IP 网络需要依靠以太网进行传输。只使用 IP 地址，报文是无法发送的。因此，在以太网上需要一种机制来提供 IP 地址和硬件地址之间的转换。这种机制就是地址解析协议(Address Resolution Protocol)。ARP 属于网络层，和 IP 处于 OSI 模型的同一层。在 IP 网络上地址解析是不断进行的，所以 ARP 报文比较适合用来检测处于混杂模式(promiscuous mode)的网络节点。

在下面的例子中，我们将讲述使用 ARP 报文是怎样解析 IP 地址的：

例如：网络上一台 IP 地址为 192.168.1.1 的 PC(X)以太网地址是 00-00-00-00-00-01，这台 PC(X)需要向网络上另外一台 IP 地址为 192.168.1.10 的 PC(Y)发

送消息。在发送之前，X 首先发出一个 ARP 请求包查询 192.168.1.10 对应的以太网地址。查询包的目的地址被设置为 FF-FF-FF-FF-FF-FF(广播)，从而本地网络上的所有节点都可以收到这个包。收到之后，每个节点会检查这个 ARP 包查询的 IP 地址和本机的 IP 地址是否匹配。如果不同，就忽略这个 ARP 包；如果匹配(Y)就向 X 发出应答。X 收到应答之后就缓存 Y 的 IP/硬件地址。然后，X 就可以向 Y 发送实际的数据。

5.检测处于混杂模式的节点

上面讲到，报文的过滤状态是处于混杂模式状态和正常的网络节点的区别。当网卡被设置为混杂模式，本该被过滤掉的报文就会进入系统的内核。通过这种机制，我们可以检测到网络上处于混杂模式的节点：我们构造一个 ARP 查询包，其目的地址不是广播地址，然后向网络上的各个节点发送这个 ARP 查询包，最后通过各个节点的回应来判断是否处于混杂模式。

下面我们讨论一下整个 ARP 请求/响应的操作过程。首先，产生一个 ARP 查询包来解析 192.168.1.10 的硬件地址。为了使网络上的所有节点都能够收到这个查询包,把这个包的目的地址设置为广播地址。理论上,只有 IP 地址为 192.168.1.10 的网卡才能对这个查询包进行响应。

进一步设想，如果我们把这个查询包的目的地址(以太网地址)设置为另外的地址,而不是原来的广播地址又将如何？例如：我们把查询包的目的地址设置为 00-00-00-00-00-01 会发生什么？处于正常模式下网络节点的以太网卡会认为这个查询包是发往其它主机的，其硬件过滤器会拒绝接收这个包；然而，如果这个网络节点(192.168.1.10)的以太网卡处于混杂模式(promiscuous mode)下，那么即使以太网地址不匹配，其硬件过滤器也不进行任何过滤，从而使这个查询包能够进入到系统的内核。因为这个节点的 IP 地址和查询包的要查询 IP 地址相同，其内核就会认为 ARP 查询包到达，应该作出应答。但是，另我们吃惊的是，这个处于混杂模式节点的内核不会应答 ARPR 查询包。这种出人意料的结果说明这个包被系统内核过滤掉了。在这里我们把这叫作软件过滤器。

再进一步，我们可以通过区别硬件过滤器和软件过滤器的不同特征来检测处于混杂模式的网络节点。硬件过滤器一般会阻塞所有无效的分组(这些分组显然不会进入系统内核)，因此能够通过硬件过滤器一般也能够通过软件过滤器，这种情况我们不多做讨论。现在我们需要构造应该被被硬件过滤器阻塞，但是却能够通过软件过滤器的报文。如果把这种报文送到各个网络节点，那么处于普通模式下的网络节点将不做应答；而处于混杂模式的节点会进行应答。

6.软件过滤器

软件过滤器依赖于操作系统的内核，因此有必要理解系统内核软件过滤器是如何工作的。Linux 是开放源玛系统，因此我们能够获得其软件过滤机制。但是对于 Micro$oft Windows 我们只有凭经验猜测了:(。

1).Linux

在 Linux 的以太网驱动模块中，分组是以硬件地址分类的。

广播包

FF FF FF FF FF FF

多投点分组

所有的分组都有一个组标志位集合，不包括广播分组。

TO_US 分组

目的地址和本机网卡相同的分组。

OTHERHOST 分组

所有目的地址和本机网卡不同的分组。

现在，我们假设具有组标志位的所有分组都是广播分组。IP 网络对应的以太网多投点分组的目的地址是 01-00-5e-xx-xx-xx，而且，通过校验组标志位本来就不能对多投点分组进行分类。这个假设并不错误，因为 01-00-5e-xx-xx-xx 是一个基于 IP 的多投点地址，但是网卡硬件地址还用于其它高层协议。

下面，我们看一下 ARP 模块的代码。

```
if (in_dev == NULL
arp->ar_hln != dev->addr_len ’ ’
dev->flags & IFF_NOARP
skb->pkt_type == PACKET_OTHERHOST
skb->pkt_type == PACKET_LOOPBACK
arp->ar_pln != 4)
goto out;
```

Linux 内核的 ARP 模块拒绝所有 OTHERHOST 类型的分组。接着，ARP 模块将处理广播、多投点和 TO_US 类型的分组。表 1 综合了硬件过滤器和软件过滤器对各种 ARP 分组的过滤处理，1 说明：hw(hardware)、sw(software)、res.(response)、gr(group)。

下面，后我们将对这六硬件地址的分组进行详细描述：

TO_US

网卡在正常模式下，所有地址为 TO_US 的分组都能够通过精简过滤器和软件过滤器。因此，不管网卡是否处于混杂模式(promiscuous mode)下，ARP 模块都会对其进行响应。

OTHERHOST

当网卡处于正常模式下，会拒绝所有地址为 OTHERHOST 的分组。即使网卡处于混杂模式(promiscuous mode)，这种分组也无法通过软件过滤器，因此这种 ARP 请求不会收到响应。