重谈 IP 欺骗技术

By papaya

阅读这篇文章之前请先了解一 TCP/IP 的基本结构和工作原理，最好在复习一下 ip spoof 常见技术，
这将有助于你更容易的理解本文。

还是先简单回顾一下吧， IP spoof 即 IP 电子欺骗，我们可以说是一台主机设备冒充另外一台主机的 IP 地址，
与其它设备通信，从而达到某种目的技术。那么该如何实现呢？很多的扫描器支持伪造源 IP 地址进行端口
扫描，这种方法是非常容易进行的，只需要构造单一的 SYN 包探测就完成了。难的是如何整个会话中进行 IP 地址伪造，

例如如何让自己成为被信任的主机去登录一台终端服务器，甚至接管已经有的会话关系。为了解决这个问题
我们可以按照由易到难的思路去实现，既然已经可以构造单一的 SYN 包那仍然可以构造第二个 ACK 包,AP 包….
等所有的应用包。理论上完全可行，但是这可是非常大的工作量。相当于用 pcap 完全自己实现 IP/TCP/应用层
协议，即使实现了网络层的通用模块，也需要根据不同的应用来继续实现高层协议。

到这里我们又可以将高级的 IP 欺骗分成两种方式，方式一是接管已经建立连接的会话，第二种是创建新的会话。

对于方式一，也是互联网上曾经盛传的 IP 欺骗方法，其中都涉及到猜解 TCP 序列号和 DOS 攻击，这里有篇文章
讲的比较详细

http://www.20cn.net/ns/hk/hacker/data/20020804015903.htm

是关于 1994 年凯文米特尼克的 IP 欺骗记录，我摘录了里面的大致过程：

1. 首先使被信任主机的网络暂时瘫痪，以免对攻击造成干扰。

2. 然后连接到目标机的某个端口来猜测 ISN 基值和增加规律！！！（重点！难点！）

3. 接下来把源址址伪装成被信任主机，发送带有 SYN 标志的数据段请求连接。

4. 然后等待目标机发送 SYN+ACK 包给已经瘫痪的主机，因为你现在看不到这个包。

5. 最后再次伪装成被信任主机向目标机发送的 ACK，此时发送的数据段带有预测的目标机的 ISN+1。

6. 连接建立，发送命令请求。

7. 擦屁股、开后门、下网、关机、睡觉。~~~zzzZZZzzz~~~

这个场景中有一个的条件是 rlogin 的地址信任关系，也就是说符合信任关系的 IP 地址进行登录是不需要密码验证的。

这个过程现在我们看起来难免会问 4 和 5 中目标机返回的数据包是如何到达攻击者机器的？因为在我们现在的
网络中攻击者伪造成信任者发送给被攻击者后，被攻击者返回的响应包 IP 是指向信任者的，即使信任者已经
被 DOS 宕机，那么这个响应包也不会发送给攻击者。

为此我们就需要考察当时的网络环境了。结论是，当时的网络拓扑和如今有着巨大差异，最大差异就是共享
环境以太网和交换环境以太网的工作方式不同。很可能当时还是其它的 token ring 等拓扑关系，我们在翻一下
以太网的发展历史。

1990 年，Kalpana EtherSwitch EPS-700 面世，网络开关(Switch)是一种提供同时多条数据传输路径的体系
结构，和电话交换机很相似，使整体吞吐量显著提高。

1993 年， Kalpana 创造了另一项突破--全双工以太网。

1994 年，大半年时间里，IEEE802.3 组都忙于其它部分的 100Mbps 以太网标准，如 100BASE-T4、MII、中继器
和全双工等标准。

1995 年 3 月，IEEE802.3u 规范被它的成员和执委会所通过，快速以太网的时代宣布来临!

1995 年 Cisco Systems 公司兼并 GrandJunction Networks 公司，提供了第一台 10Mbps 工作组交换器。通过
这段历史可以了解到交换设备的工业化进程是在 1995 年才开始的，所以前面这个故事基本可以断定
发生在共享环境中。

那么交换环境里如何实现呢？知道共享环境和交换环境的差异之后这个问题就不难解决了，通过 ARP/CAM/STP
等等方法想办法获取 4 ，5 步骤中返回的数据就可以了。当然这些都是理论的东西，目前并没有见到很实用的
工具出现。（我也纠结在如何实现一个通用的 Hijacking an Authorized Session tool）。

谈谈方式二，我们有新的方法来快速实现，就是基于代理的 IP 欺骗方法，快速创建伪 IP 会话。

云舒曾在 http://icylife.net/yunshu/show.php?id=732 重提到特殊环境的 IP 欺骗，方法好但是实现相对繁琐，
原因还是相当于完全自己实现 IP/TCP/应用层协议。下面我们就展开讨论基于代理的 IP 欺骗方法。这种方法
仍然需要 ARP/CAM 或者其他欺骗方式的支持，原因稍后会提到，且只能在同一个子网内（严格来说是同一个
广播域）。通过一个实例来讲解一次 IP 欺骗流程，场景中有攻击者 A，受信任者 B，服务器 C。

第一步
A 中的 IE 访问一个不存在的 IP 地址 http://1.1.1.1/ip.asp，正常情况下将不会有任何回应。

A 中我们抓取并修改刚才这个发往 1.1.1.1 数据包的目标 IP 为 C， 源 IP 为 B，目标 MAC 为 C 后重发。

A 中启动一个 ARP 线程刷告诉 C，B 的 ip 地址对应的 MAC 是 A。

第二步
C 收到原 IP 为 B 的数据包后做出响应，目标 IP 为 B,目标 MAC 为 A。

第三步
A 收到 C 发往 B 的响应包，修改此包目标 IP 为 A，原 IP 为 1.1.1.1 后重发给 A

A 收到重发的数据，对于 A 中 IE 来说，发送给 1.1.1.1 请求并得到了来自 1.1.1.1 的回应，IE 会接受并处理这个数据包。

至此 IP 欺骗完成，上面的流程使攻击者可以伪装成任意的子网 IP 地址取得服务器 C 的信任。

如何伪装成外网的 IP 地址呢？很简单，用第一步中的 ARP 线程刷 C 的 IP-MAC 关系为 a.ip=gate.mac，这样就
可以实现在同一内网伪造任意的 IP 地址。

通过上面两步中可以看到我们无需关心 TCP 序列号，无需关心信任者的存活状态，无需关心上层协议，可应用
于 RDP,FTP,SSH,HTTP 等任何 IP 协议。通过测试我们也证实了本文的可行性。

而达到这个效果只需要几句关键的代码就可以实现：

```
int strindex = 0;
string Desmac = Function.GetMACAddress(s, ref strindex);
int Index = 26;
string Srcip = Function.GetIpAddress(s, ref Index);
string Desip = Function.GetIpAddress(s, ref Index);
```

//基本解析

```
if (Srcip == MyLocalHost.ip[0] && Desip==tagip)
```

//如果是要转发的数据包，例如发往 1.1.1.1

```
                {

                    //修改原 IP 为受信任人 IP 和目的 IP 和目的 MAC 为真实
目标后转发
                    Index = 26;
                    Function.Setipaddres(ref s, psrcip, ref Index);
                    Function.Setipaddres(ref s,tagetip, ref Index);
                    modifydesmac(s, tagetmac);
                    CnCerT.Net.Packet.DoCheck.CheckIP(ref s);
                    CnCerT.Net.Packet.DoCheck.CheckTCP(ref s);
                    mypcap.SendPacket(s);

                }
                else if (Srcip==textBox_targetip.Text &&
Desip==textBox_srcip.Text)//如果是目标返回的数据包
                {

                    //修改原 IP 为受信任 IP，目的 IP 为本机后重发
                    Index = 26;
                    Function.Setipaddres(ref s, tagip, ref Index);
                    Function.Setipaddres(ref s, MyLocalHost.ip[0], ref
Index);
                    CnCerT.Net.Packet.DoCheck.CheckIP(ref s);
                    CnCerT.Net.Packet.DoCheck.CheckTCP(ref s);
                    mypcap.SendPacket(s);
```

在不能进行 ARP 欺骗的环境中可以结合 CAM 欺骗方式进行 IP 欺骗，具体的细节读者可以参考《无 ARP 欺骗的嗅探技术》
继续进行研究，本文探讨到此。

通过杜绝 ARP/CAM/STP 欺骗可有效防护本文提到的攻击方法和工具。

References:

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html
http://www.securityfocus.com/infocus/1674
http://staff.washington.edu/dittrich/papers/IP-spoof-1.txt
http://blog.csdn.net/ecrown/archive/2005/01/12/249740.aspx