Author:bugcx or Anonymous
Url:
http://blog.bug.cx/2012/04/25/%e5%9f%ba%e4%ba%8earp%e6%ac%ba%e9%aa%97%e5%86%85%e7%bd%91%e6%l
(撸一撸) | bugcx's blog | 关注网络安全

摘 要 本文从协议欺骗的角度，讨论了在内网中进行网络渗透的方法，研究了基于ARP欺骗的数据包替换技术，以替换WEB回复报文中的链接信息为例，分析了无漏洞渗透技术的原理。在此基础上，探讨了基于ARP欺骗的内网渗透的防范措施。
关键词 ARP欺骗；内网渗透；无漏洞渗透防范

协议欺骗是指通过对通信双方使用协议弱点的利用，冒充其中一方与另一方进行通信的行为。对于广播式网络，只要更改自己网卡的接收模式为混杂模式，理论上就可以截获所有内网上的通信。对于交换式网络环境，如果要截获网络上不属于自己的通信，可以通过协议欺骗来实现。内网渗透指的是在网络内部的渗透，在本地局域网内部对网内的其他系统进行渗透的过程。基于ARP欺骗的内网渗透指网络攻击者利用ARP欺骗截获不属于自身的通信，并从这一条件中获取更多利益的行为。

ARP（Address Resolution Protocol，地址解析协议）是一个位于TCP/IP协议栈中的低层协议，负责将局域网中某个IP地址解析成对应的MAC地址。

IP地址到MAC地址的映射关系主要是靠ARP协议来实现的。对于网络主机，这个映射关系存放在ARP高速缓存中。ARP协议是这样工作的：首先，网络通信源机器向网络广播ARP请求包，请求网络通信目的机器IP所对应的MAC地址；然后使用该IP的机器会向请求方发送一个含有其MAC地址的ARP回应包，这样请求方就知道向哪个MAC地址（目的主机）发送数据。

ARP协议存在以下安全问题[1]：无连接、无认证、动态性、广播。利用ARP协议的这些安全问题，可以设计ARP协议欺骗的步骤和方法。

① 主机在不知道目的IP对应的MAC地址时，进行ARP广播请求，入侵者可以在接收到该ARP请求后以自己的MAC地址应答，进行假冒；

② 由于被假冒机器所发送的ARP应答有可能比入侵者发送的应答晚到达请求主机，为了确保请求主机的缓存中绝大部分时间存放的是入侵者的MAC地址，可以在收到ARP请求后稍微延迟一段时间再发送一遍ARP应答；

③ 有些系统会向自己缓存中的地址发送非广播的ARP请求来更新自己的缓存。在交换网络环境下，如果请求主机缓存中已存有正确的主机MAC地址，入侵者就不能用以上接收请求然后应答的方法来更换被攻击主机缓存内容。由ARP弱点分析可知，应答可以随意发送，不一定要在请求之后。

基于协议欺骗的内网渗透技术也称无漏洞渗透技术。无漏洞渗透技术是相对于利用软件漏洞进行网络渗透的技术来说的。在以太网中，只要被渗透机器在网络中传输的数据包经过本地网卡，在本地就可以截获其数据包中的敏感信息，并可以更改数据包内容、替换数据包中的传输实体，使得被渗透机器上的敏感信息泄露，并可以使其在接收到被更改过的数据包之后，产生更多的损失。对内网中的机器进行渗透，不一定需要软件漏洞的存在。将这种不需要软件漏洞进行渗透的技术称为无漏洞渗透技术。

在交换型以太网中，所有的主机连接到交换机，交换机知道每台计算机的MAC地址信息和与之相连的特定端口，发给某个主机的数据包会被交换机从特定的端口送出，交换机通过数据包中的目的MAC地址来判断最终通过自己的哪个端口来传递该报文，通过ARP欺骗之后，交换机将无条件地对这些报文进行转发，从而确保了ARP欺骗报文的正确发送。

无漏洞渗透技术的研究重点是在欺骗成功之后，对数据包的处理。对数据包处理的方式主要有两种，敏感信息的截取和传输实体的获取与替换。

·报文中敏感信息的获取

对于明文传输的面向连接和非面向连接的协议，在截获报文之后，对报文中传输的信息进行还原，并提取其中的敏感信息，如非加密WEB页面的用户名、密码，TELNET的用户名、密码，FTP的用户名、密码和与邮件服务器进行交互时所需要的用户名、密码等都可以直接进行嗅探。

·传输实体的获取与替换

明文传输的面向链接的协议中有很多协议支持文件实体的传输。如HTTP协议、FTP协议、SMTP协议。对文件的实体获取是相对简单的，对到达本地网卡的报文进行缓存，当收到连续报文中小于1500Byte[2]的报文时对报文进行还原，文件实体便可以得到。

本文以网页传输为例，来探讨传输报文中网页里包含链接的替换，分析WEB欺骗攻击[3]的原理。

数据包常规的传输路径依次为网卡、设备驱动层、数据链路层、IP层、传输层、最后到达应用程序。而包捕获机制是在数据链路层增加一个旁路处理，对发送和接收到的数据包做过滤/缓冲等相关处理，最后直接传递到应用程序。值得注意的是，包捕获机制并不影响操作系统对数据包的网络栈处理。对用户程序而言，包捕获机制提供了一个统一的接口，使用户程序只需要简单的调用若干函数就能获得所期望的数据包。目前，在Unix下有Libpcap开发包、Windows下有Winpcap开发包，都可以轻松地实现数据包的捕获和分析。

·WEB请求截获

通过浏览器发送WEB页的请求，经过封装后形成的以太网数据包不会超过1514Byte，所以，不用担心WEB请求报文会出现分片的情况。当实现欺骗之后，就不断地截获、转发两个被欺骗目标之间的通信报文，并分析每一个小于1514Byte（以太包）的通信报文。

一个HTTP请求包包含14字节的以太网头部、20字节的IP头部和20字节的TCP头部以及HTTP请求包。其中HTTP协议（以HTTP1.1为例）包格式[4]如图1所示。

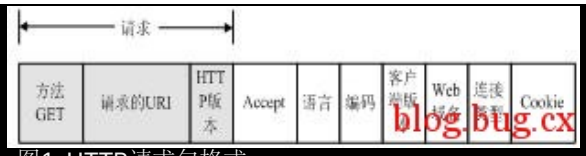

图1 HTTP请求包格式

一个请求包括：方法＋请求URI＋HTTP版本号。方法有：GET|HEAD|POST|扩展方法；URI＝目录与文件名；HTTP版本为HTTP/1.1。一个完整的URL为协议类型＋WEB域名＋URI。截获到HTTP请求包之后，发送以自身为源IP的伪造请求包到WEB服务器，和WEB服务器交互，以获取所有请求的文件内容。注意，在截获请求后，需要缓存TCP头部的序号和确认号，以备发送修改后的请求文件所用。

·获取正常WEB页、替换连接

复制请求的内容，根据序号和确认号构造包头，发送到WEB服务器。缓存头部信息和获取的文件内容。并在每收到一次来自WEB服务器的TCP包时，即构造并发送一个确认给WEB服务器，直到缓存了所有的页面文件内容。将获取的页面内容进行更改，替换其中的链接（以替换页面的所有链接为例）。这需要对HTTP回应包进行分析。

图2 HTTP协议回应包格式

如图2所示，从以太帧中剥离的HTTP回应包格式包含协议版本、状态码、服务器版本、请求文件相关属性和请求的文件内容。紧跟着回应包的下一个传输的文件内容直接跟在TCP头部之后。

在缓存之前，先对文件内容中的链接信息进行更改，将链接信息替换成自己想要换成的URL。并将信息存入一个文件，当所有的内容接受完毕形成一个文件之后，需要利用在截获HTTP请求时缓存的序号和确认号构造报文发往被欺骗者。

·发送伪装数据包

在构造HTTP回应包时，需要填充整个以太帧。不需要从头开始去构造整个包，在前面获取到来自WEB服务器的回应包时，已经将包头部分进行了缓存，需要修改和构造的部分有：IP头部校验和、TCP头部中的序号和确认号、TCP头部校验和[5]、HTTP协议回应包中的“状态码”、“最后修改时间”、“文件长度”字段、文件信息的填充。

一次完整的ARP欺骗及渗透过程如图3所示。

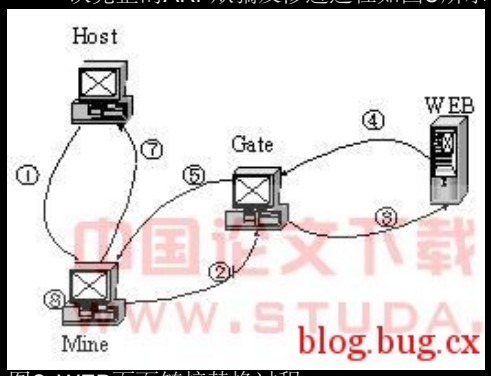

图3 WEB页面链接替换过程

Host、Mine、Gate同在一个交换式局域网内，Gate为局域网网关。通过ARP欺骗，Mine截断Host与Gate之间的报文传输，当Host请求Web页面时：

① Host发送请求报文；
② Mine截获并提取出URL，模拟HTTP请求发送报文到Gate；
③ Gate转交报文到Internet上的WEB服务器；
④⑤ WEB服务器发送HTTP响应及数据包到Mine；
⑥ 缓存了所有文件后，对文件中的链接进行替换；
⑦ 将替换后的文件发送到Host。

在被欺骗者接收到一个被篡改的网页之后，它的网络行为将完全与预先设计好的虚假站点进行交互，从而可以进行更进一步的渗透。

在交换式网络中防范ARP欺骗主要有以下几种方法：

·使用静态ARP表

在关键设备如网关、防火墙和边界路由器等设置静态的ARP，不要让系统刷新设定好的ARP转换表。在图3中，在网关Gate中使用静态ARP表，则可以避免通过网关进行ARP欺骗。

·使用ARP服务器

在内部网络中设置ARP服务器，通过该服务器查找自己的ARP转换表来响应其他机器的ARP广播，而禁止其他系统响应ARP请求。

·定期轮询

管理员定期轮询（可通过软件实现）网络内部的IP地址与MAC地址的对应关系，通过与已有记录的比较来发现ARP欺骗。

·主动出击

主动出击，用一些安全工具（如AntiArpSniffer）在网络中进行检测，可以检测到本地网络上的ARP欺骗报文。

·使用加密通信

无漏洞渗透的报文中敏感信息的获取和传输实体的替换主要针对非加密通信，将内网的通信进行加密可以有效地防止这类攻击。例如在内部网络利用共享来传递文件时，首先用加密工具（如WinRAR）对文件进行压缩加密；内部网的系统登录用SSH替换Telnet；用SFTP替

换FTP；内部网站访问用HTTPS替换HTTP等等。

·划分虚拟局域网

欺骗攻击无法跨网段工作，将网络进行越细致地分段，无漏洞渗透成功的可能性就越小。将受信任主机设置在同一社区VLAN中，将绝密性主机设置在隔离VLAN中，可以有效地防止无漏洞渗透的渗入。

·提高防范意识

目前，很多容易被攻击者注意的网站（如，网络银行等），都采用了HTTPS代替了HTTP协议来传输网页和交易数据，已经避免了这类攻击发生的可能。但对于那些没有采用加密通信的WEB站点来说，WEB链接替换攻击依然有成功的可能。对这种攻击可以从浏览器终端用户的角度来防范，使用一些较为安全的浏览器来访问网站，如GreenBrowser，可以设置从网页链接跳转到非本网站网页时给出提示，在发生此攻击的时候，可以很容易发现。

上文研究了基于ARP协议欺骗的内网渗透，可看出在内网中即使攻击者没有掌握网络内部任何操作系统或应用软件的漏洞，但是利用协议的弱点，还是可以在内网中进行渗透攻击获取利益。在加强网络边界防护的同时，不能忽视网络内部的防护。

[1] 秦相林.二层交换网络上的嗅探技术研究[J]，自然科学报，2005
[2] 基于IP分片的攻击方法[EB/OL]，HTTP://www.99net.net/study/safe/92510429.htm，2003
[3] Edward W. Felten. Web Spoofing: An Internet Con Game[C]，Princeton University，1997
[4] RFC2616:Hypertext Transfer Protocol -- HTTP/1.1[S]，1999
[5] SYN Flood攻击的基本原理及防御[EB/OL]，http://shotgun.patching.net/syn.htm，2001

最新文章 相关文章 热评文章 Waiting Waiting