防火墙攻击穿透技术研究与实现

The Research and Implementation of the Attacking and Penetrating Firewall Technologies

胡善岳 张新泉 李治云 吴 娅 (96623 部队 40 分队 江西省上饶县 334000)

摘要:本文首先对防火墙的典型攻击技术——IP 地址欺骗技术进行了分析;在分析研究了 ICMP 协议的基础上,利用 ICMP 协议的特点研究并实现了防火墙的 ICMP 隐蔽通道攻击穿透技术。

关键词:防火墙 攻击穿透 ICMP

1 引言

目前,防火墙技术已从简单的包过滤技术发展到具有智能性的状态检测技术。但一直以来,网络安全事件非但没有减少,反而在增加,其中一个重要原因就是黑客不断的在研究网络的攻击技术和手段,尤其是防火墙的攻击穿透技术。本文从网络战的角度出发,也对防火墙的攻击穿透技术进行了研究,本文利用 ICMP 协议自身缺点研究并实现了 ICMP 隐蔽通道攻击穿透技术,其目的不是为了去攻击和破坏网络,而是一方面为了更好地防护好己方网络的安全,另一方面是为了在今后的网络战中,能够对敌方网络系统进行有效攻击。

2 典型的防火墙攻击穿透技术研究

防火墙攻击穿透技术是黑客和网络安全专家一直在研究的技术,其攻击的手法和技术越来越智能化和多样化。但是就攻击穿透防火墙的过程上看,大概可以分为三类:

(1) 是探测在目标网络上安装的是何种防火墙系统并且找出此防火墙系统允许哪些服务,即为防火墙的探测攻击。

(2) 是采取地址欺骗、TCP 序号攻击等手法绕过防火墙的认证机制,从而对防火墙和内部网络进行攻击。

(3) 是寻找、利用防火墙系统实现和设计上的安全漏洞,从而有针对性地发动攻击,此种攻击难度比较大,可是破坏性很大。

本文主要分析的是攻击穿透防火墙技术最常用也是最基础的技术:IP 地址欺骗攻击穿透技术。IP 地址欺骗攻击穿透技利用了 IP 协议自身的缺点,IP 协议依据 IP 数据报头中的目的地址来发送 IP 数据包。如果目的地址是本地网络内的地址,该 IP 包就被直接发送到目的地;如果目的地址不在本地网络内,该 IP 包就会被发送到网关,后由网关决定将其发往何处。从中可以看出 IP 路由 IP 包时对 IP 报头中提供的 IP 源地址不作任何检查,并且认为 IP 报头中的 IP 源地址即为发送该数据包主机的 IP 地址。当目的主机要与源主机进行通讯时,它以接收到的 IP 包的源地址作为其发送 IP 包的目的地址,来与源主机进行数据通讯。

IP 的这种数据通讯方式虽然非常简单和高效,但它同时也是 IP 的一个安全隐患,因为 IP 地址可以被伪造。我们可以伪造 IP 发送地址来产生虚假的内部数据分组,只要系统发现发送地址在其自己的范围之内,则它就把该分组按内部通信对待并让其通过,从而本应被防火墙拦截的数据包能够顺利通过防火墙到达目的主机。

具体的过程可以简单的用图 1 进行说明:

C(B) - - - - SYN - - - - > A

B < - - - - SYN + ACK - - - - A

C(B) - - - - ACK - - - - > A

C(B) - - - - PSH - - - - > A

图 1 IP 地址欺骗攻击过程图

图中 C 是攻击机,其目标是假装 B 主机与 A 主机

进行通信。我们将从 C 主机发送数据的报头中的 IP 地址改为 B 主机的 IP 地址，让 A 主机错误地认为是 B 主机发送来的数据包。由于 TCP/IP 协议真正要建立起通信，必须经过二次握手，所以在此过程中首先采用一定的攻击手段让 B 主机瘫痪，然后猜测 B 主机的应答序列号，如果序列号猜测正确，则很容易建立连接，从而达到了欺骗攻击的目的。

3 ICMP 隐蔽通道攻击穿透技术研究

上文分析的 IP 地址欺骗攻击穿透技术对于包过滤型防火墙是可用的，但对于其它类型的防火墙就没有作用。ICMP 隐蔽通道攻击技术是在深入分析研究了 ICMP 协议的基础上，利用 ICMP 响应应答报文作为秘密数据传输的隐蔽通道（即是非法程序利用那些本来不是用于通信目的的途径来进行通信的途径），从而实现对防火墙的攻击穿透。

3.1 ICMP 隐蔽通道攻击技术原理

ICMP 是互联网控制报文协议（Internet Control Message Protocol）的简称，其主要用途是向 IP 和高层协议通报有关网络层的差错和流量控制情况，目的是返回关于网络问题的诊断信息。ICMP 报文的类型有很多，几种常用的报文类型如表 1 所示。

表 1 ICMP 报文类型表

报文类型	描述	报文类型	描述	报文类型	描述
0	响应－应答	8	响应－请求	14	时间戳应答
3	目的地不可达	11	超时	15	信息请求

ICMP 报文由报文头和报文体两部分组成，报文头主要由类型字段、代码字段与校验和字段等构成。其中类型字段为单字节整数，表示差错的类型；代码字段为单字节整数，表示差错的原因，类型字段和代码字段规定了报文的意义和该种报文的分组格式；校验和表示整个 ICMP 报文的校验结果。

在所有的 ICMP 报文类型中最有利用价值的类型是 0x0（响应应答报文）和 0x8（响应请求报文），Ping 命令就是利用这两种类型报文来完成工作的。工作时，Ping 命令向远程主机发送一个或多个 ICMP_ECHO 数据包，其目的是判断远程主机是否可以到达。ICMP_ECHO 数据包的选项域部分可以填写数据，通常是用来记录 ICMP 报文到达远程主机的过程中，沿途经过的路由器地址及其耗费的时间。通常情况下，很少有设备检查这个字段中的内容，这就给隐蔽通道的建立提供了理想的场所。

源主机在发送 ICMP_ECHO 报文时，在 ICMP 数据包包头的选项域（Option Data）中，可以添加任何数据，这些数据是用来反映网络状况（比如：延时、路由器地址等等）的。当目标主机收到 ICMP_ECHO 报文后，在 ICMP 响应应答报文中填写标识域和序号域以回应响应请求报文，并且把响应请求报文数据包中选项域的数据原封不动的返回去。据此我们把要发送的数据隐藏在 ICMP 数据包的包头选项域中，并将其伪装成响应应答数据包，这样就建立了隐蔽通道。正常情况下，防火墙及其它安全设备都不会检查 ICMP 报文中的内容，因此隐蔽通道很容易穿透网络安全设备的阻拦。

即使在一些防护措施比较严密的网络中，防火墙对 ICMP 报文进行过滤（如 ICMP 响应请求报文），但 ICMP 响应应答报文和 ICMP 目的地不可到达报文往往不在过滤策略之中，这是因为一旦不允许这两种报文通过就意味着主机没有办法对外进行 Ping 的操作，并且当访问某一不存在的网站或要访问的网站的路由有问题时，就会很长时间没有回应，这样既不便于网络的安全管理，也不便于网络本身的运行需要。所以将要发送的数据隐藏在 ICMP 响应应答报文或 ICMP 目的地不可到达报文的包头选项域中，通过隐蔽通道进行数据的传输就可以很容易的穿透防火墙。

3.2 ICMP 隐蔽通道攻击技术设计

ICMP 从 OSI 参考模型上来看是属于 IP 层，但它却与 TCP/UDP 一样用 IP 协议对数据包进行封装并发送。ICMP 属于网络层的特性使得 ICMP 报文在传输时有一个很大的特点就是不用端口，只要有目的地址即可，ICMP 报文的另一个特点就是它是无连接的，即只要发送端完成 ICMP 报文的封装并传递出去，它就会象邮包一样自己寻找目的地址，这使得 ICMP 数据包非常灵活快捷，但同时也很容易被伪造，本文利用 Raw Socket（原始套接字）编程技术直接改写报文的 ICMP 首部和 IP 首部。Raw Socket 允许程序绕过 TCP/IP 传输层直接访问底层协议（如 ICMP 等），所以 IP 层的封装工作是用手工填充的方法实现，而不是由操作系统自动完成。

本文设计的隐蔽通道攻击技术实现程序是用 ICMP

响应应答报文来作为秘密数据传输的隐蔽通道的。隐蔽通道实现程序由两部分组成:接收程序和发送程序。

利用系统内核自行处理 ICMP 报文的特性,将接收程序伪装成一个 Ping 进程,这样不仅实现了接收程序自己的隐藏,而且同时也获得了 Ping 进程的处理权。当主机接收到 ICMP 报文时,接收程序首先判断 ICMP 报文的类型,如果是 ICMP 响应应答报文(类型值为 0),则再进一步判断是不是用于实施攻击的报文,如果是(判断是通过响应应答报文中的 icmp_seq 字段中预先设定的特定值来实现的),则进行接收处理并解出可选数据字段中的数据和代码,然后根据此数据和代码执行相应的攻击动作(如格式化磁盘、停止进程或重启系统、执行特定的程序等等);如果不是,则将该报文交由正常的系统 Ping 进程处理。

接收程序的算法实现设计如下:

(1) 程序处于运行监听状态;

(2) 接收 ICMP 报文,然后判断 icmp_type 字段中的类型值,若不为 0,则转(1);

(3) 判断 icmp_seq 字段中的特征值,若不是预先设定的特定值,则转(1);

(4) 解出可选数据字段中的数据和代码,并据此执行相应的攻击动作;

(5) 转(1)。

对发送程序,利用 Raw Socket 技术,在传输数据前对数据包进行伪装和填充,将 ICMP 的数据类型设为 0x0,即表明数据包中是有效的 ICMP 响应应答信息,这样就可以成功欺骗防火墙。同时在 icmp_seq 字段中填入的是设定的特定特征值,而不是响应请求报文包的序列号;在可选数据字段中填入的是要发送的数据和代码。

发送程序的算法实现设计如下:

(1) 构造 ICMP 报文,并设定 icmp_type 字段中的值为 0;

(2) 填充 icmp_seq 字段中的特征值和可选数据字段中的数据和代码;

(3) 封装成 IP 数据并发送;

(4) 判断数据是否发送结束,若没有则转(2);否则程序结束。

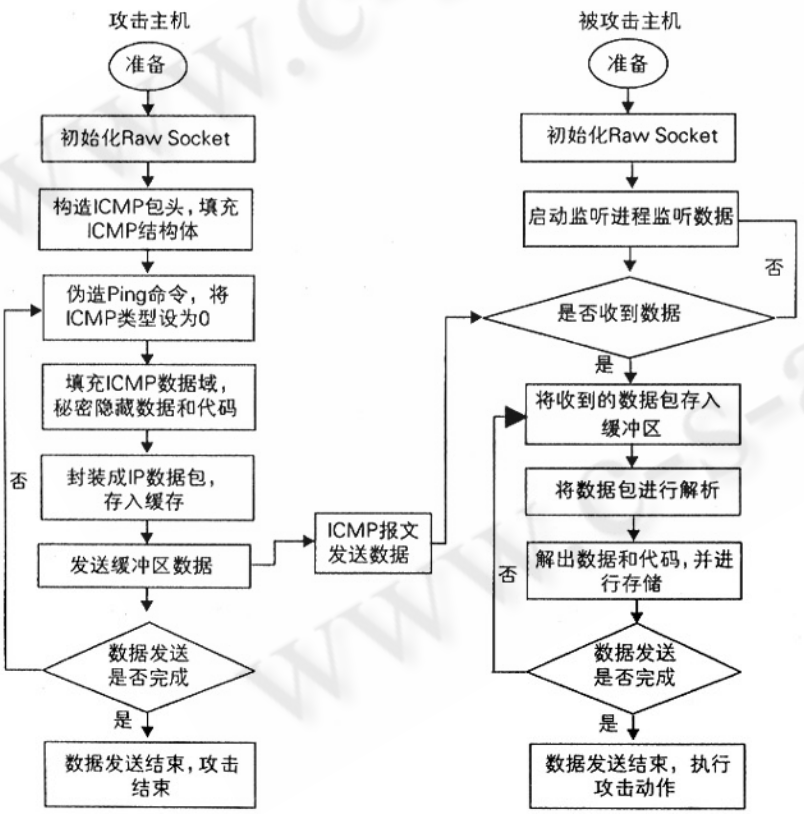

图 2　隐蔽通道攻击程序实现流程图

3.3 ICMP 隐蔽通道攻击技术实现

根据以上算法,本文利用 Windows Sockets 套接字编程技术实现了该隐蔽通道传输秘密数据的程序。Windows Sockets 为 Microsoft Windows 操作系统环境定义了一种编程接口,它使用由美国加州大学在 Berkeley Software Distribution(BSD)中提出的"套接口"概念。套接口是网络中可以被命名和寻址的通信端点,从应用程序的角度来看,它是操作系统分配的一种资源,用一个称为套接字的整数表示,基于 TCP/IP 协议和 Windows Sockets 我们可以编制出各种网络通信应用程序。

隐蔽通道攻击程序由发送程序和接收程序两部分组成,发送程序(Send. exe)由攻击主机执行,接收程序(Accept. exe)由被攻击主机执行。其程序实现框图如图 2 所示。

(下转第 60 页)

(上接第 56 页)

4 ICMP 隐蔽通道攻击穿透技术防范

ICMP 隐蔽通道攻击穿透技术本质上是针对 ICMP 协议本身的特点而研究实现的一种防火墙攻击穿透技术,所以对该攻击穿透技术最好的防范方法是在网络中禁止 ICMP 协议的报文通过,当然,这样对网络管理和运行都会带来一定的不便。要很好地防范利用 ICMP 隐蔽通道攻击穿透技术实现的网络攻击,就应对进出网络的数据包尤其是从外网到内网的 ICMP 协议数据包进行监控和分析,一旦发现有异常的 ICMP 协议数据包或本来不该有的 ICMP 协议数据包出现,就要立即采取措施,因为这很有可能就是利用 ICMP 隐蔽通道攻击穿透技术而实现的网络攻击报文。

5 结束语

目前防火墙技术是网络安全防护技术中最常用的技术,防火墙产品也是网络防护设备中最常用的防护设备。在网络安全事件日益增多的今天,从防护者的角度对网络攻击技术尤其是防火墙的攻击穿透技术进行研究,对于我们更好地保护好已方网络,更好地防止网络安全事件的发生有重要意义。

参考文献

1 孟朝霞、吴晨晖, ICMP 的应用、缺陷及防御,运城学院学报,No. 3,21 – 22,2003。

2 周炎涛、李立明, TCP/IP 协议下网络编程技术及其实现,航空计算技术,No. 3,122 – 124,2002。

3 陈康荣,防火墙穿透方法初探,计算机安全,No. 8,32 – 34,2003。

4 宋海涛、宋如顺,网络秘密信道机理与防范,计算机工程,No. 8,120 – 122,2004。

5 宿 洁、袁军鹏,防火墙技术及其进展,计算机工程与应用,No. 9,147 – 149,2004。