Internet 攻击和防火墙新技术

汪立东 (哈尔滨工业大学 150001)
钱丽萍 (内蒙古大学计算机系 010021)

摘要:随着 Internet 应用的普及,其安全性问题也日渐突出。本文介绍了 Internet 常见攻击的原理与防范及当前防火墙采用的一般技术,提出了将来防火墙设计中可能采用的一些新技术,包括内核级透明代理、增强的用户认证机制、多防火墙间互操作能力、虚拟专用网支持、多媒体应用支持、内容和策略感知能力、智能型日志和审计系统等。

关键词: Internet 攻击 网络安全 防火墙 过滤 内核代理 强用户认证

一、Internet 常见攻击与防范

Internet 的安全问题主要源于以下几方面:

(1)作为 Internet 基石的 TCP/IP 协议本身在安全性方面的缺陷;

(2)各种应用程序中包含的漏洞和 Bug;

(3)网络管理员及用户的安全意识差;

(4)社会原因,如信息间谍的存在和公众对黑客才智的赞赏等。

Internet 常见的网络攻击大致有以下几类:

1. **嗅包**(Sniffing)

嗅包是利用以太网的广播特性(CSMA/CD(Carrier Sense Multiple Access with Collision Detect:带碰撞检测的载波侦听多路访问协议)),用软件在原以太设备上侦听或通过将网络接口置为混杂模式(Promiscuous Mode)接收进出本网段的所有 MAC 包。由于 Internet 上的信息通常是明文传输的,当发现了满足一定条件的包,则可将其内容记入一文件或进行其他操作(如劫持,拒绝服务等)。最一般的规则是包中包含诸如 login 或 password 之类的词,通过捕获 FTP 或 TELNET 包的前 128 个字节即可实现。嗅包程序(Sniffer 嗅包器)也可用来作为网络测试工具,如 SUN Solaris 上的 snoop 命令。嗅包是黑客攻击网络的主要方法之一,很多嗅包器可以从网上的匿名 FTP 服务器上找到。常见的嗅包器有 HP/UX 和 Sun OS 上的 nfswatch, DOS 的 Ethload, Machintosh 的 Etherpeek。Esniff.c 和 sniffit 是黑客常用的嗅包程序。嗅包器的快速传播给网络安全带来了极大的危害。利用嗅包攻击的目的主要是:获得帐号和口令,获得敏感数据,冒充和劫持等。可以使用强用户认证机制及一次性口令避免口令被嗅;用加密传输避免数据被捕获;使用 Hub 分隔网段;采用 VPN(Virtual Private Network)技术等。

2. **冒充**(Spoofing)

冒充是指一主机以另一主机的名义进行操作。被冒充的信息包括 IP 地址、域名、E-mail 帐号等,可以通过修改 IP 地址、域名、路由信息等实现。最常见的是冒充内部网主机地址而试图通过代理进入内部网,即所谓的源地址冒充,可以在路由器上滤掉所有目的地址和原地址均是内部地址的包来防范这类冒充。再如冒充 E-mail 地址发信:先登录到欲冒充主机的端口 25(smtp 端口),设欲冒充的帐号为 swan@victim.hit.edu.cn,收信方为 hawk@dest.hit.edu.cn,则如下操作将产生一个假源地址的 mail:

```
$ telnet victim.hit.edu.cn 25
HELO victim.hit.edu.cn
MAIL FROM: swan@victim.hit.edu.cn
RCPT TO:hawk@dest.hit.edu.cn
DATA
< 信件内容.....>
.
QUIT
```

这在大多数未实现 RFC 931 的 UNIX 系统上好使,但只要细心查看 mail 头信息,就会发现还是有所不同。防范冒充攻击,最常用的是防火墙,可结合包过滤及在代理中进行 IP 地址、域名等的交叉检验机制实现。其他的方法如包戳记、包签名等。

3. **特洛伊木马**(Trojan Horse)

特洛伊木马是一个独立的程序,看起来完成某一功能,实际执行另一功能。比如做一个假的登录界面来骗取他人登录时的帐号和口令。当黑客设法进入系统后,他们会清理现场,留下暗门以备后用再退出。通常是用

一个带激活条件的木马程序代替系统中某个程序。当条件满足时，此木马程序被激活，使攻击者可以再次进入系统。比如攻击者编写了一个程序替代 Unix 系统中的 in.fingerd，当 finger 此机器时，它检查所 finger 的是否是一个事先设好的用户号，若不是，则执行正常的 finger 功能；若是，则打开/etc/passwd 文件，向其中追加一个用户。只要/etc/inetd 中 finger 的运行者为 root，则就可以追加一个不用口令却具有 root 权限的帐号。由于系统中程序众多，木马的隐蔽性强，管理员很难发现。防范特洛伊木马关键是要配置好系统，防止系统被入侵，并要慎用免费软件。

4. **拒绝服务攻击**(Denial of Service)

这类攻击的特点是使得服务器不能为客户提供良好的服务。实施这类攻击的方法较多。如：

(1)**逻辑炸弹**：通过不断地向服务器发送连接请求，使服务器忙于应付，最后只得关闭服务。如不断地向一个电子信箱发送邮件；与 telnet 服务器建立尽可能多的连接导致其无法承受而 down 机。由于网上有许多炸弹，如 teardrop 及其变形，其使用简单，现在经常有服务器和主机被炸。可过滤掉不信任地址及用代理型防火墙防范。

(2)ICMP 包攻击：攻击者将 ICMP 包送到一个主机或路由器，告诉它们停止发送数据。可利用防火墙，过滤或忽略 ICMP 包。

(3)TCP 包的序列数攻击：TCP 是面向连接的协议，比 UDP 更安全。TCP 连接双方用序列数来协商以建立连接和进行正确的数据传送。当 TCP 序列数可能被猜测，TCP 包也可能被捕获而获得序列数，由此可以劫持已建立的连接或破坏 TCP 连接建立过程中的三次握手迫使断连。可以使用加密序列数或随机序列数来防范序列数攻击。

(4)ICMP 包洪泛：若 ICMP 包包头中 ICMP-ECHO 域置位，则收到此包的主机都会发回一个响应(ICMP-ECHOREPLY)包。如果不断地向一台服务器发出 ICMP-ECHO 包，则服务器忙于 ICMP 响应而影响了对正常请求的响应。再如冒充欲攻击的主机的地址，向一个大的网段的所有主机发出 ICMP-ECHO 包，则那个网段中的所有主机都会向被冒充的主机发 ICMP 响应包，以此挤死被冒充的主机。可以用防火墙滤掉或丢弃 ICMP-ECHO 请求包。

5. **NFS 和 NIS 攻击**

NFS(Network File System 网络文件系统)通过让客户 mount 一个磁盘到一远程服务器上而允许系统在一个网络上共享文件。在系统配置方面很容易失误，使黑客也可能通过 NFS 而 mount 上来，或通过劫持一个已存在的 NFS mount 来访问系统。NFS 的用户认证能力很弱，当 NFS 工作时，客户机可以读写服务器上的文件，却不用登录到服务器或输入口令，且 NFS 不记录处理信息，使管理员更不易发觉。

NIS(Network Information System 网络信息系统)维护着包含口令表、用户组文件、主机表和网络可共享的其他信息的一个分布式数据库。NIS 多用于分配口令信息，多数 NIS 的实现对哪台机器能请求信息完全没有控制，只要攻击者能猜到 NIS 的域名，则能送一个 NIS 请求到 NIS 服务器，可以获得口令信息的完整拷贝(包括加密的口令)，即使运行了 shadow 口令也不行，它们也可能被 Crack 掉。

防范：NFS 和 NIS 有其安全方面的漏洞，应尽可能不提供 NIS，避免使用 NFS，若要使用，则应在防火墙内部使用。

二、防火墙的概念

防火墙是设置在内部网络与 Internet 之间的一个或一组系统，用以实施两个网络之间的访问控制和安全策略。狭义上防火墙指安装了防火墙软件的主机或路由器系统；广义上还包括整个网络的安全策略和安全行为。防火墙从结构上可分为屏蔽路由器(Screened Router)、双穴主机(Dual-home host)、屏蔽主机(Screened Host)、屏蔽子网(Screened Subnet)、混合网关(Hybrid Gateways)等；从运行机制上，主要有过滤型防火墙(Filtering Firewal)、电路层网关(Circuit Gateway)、代理服务器(Proxy Server)。

过滤型防火墙工作在网络层，基于单个包实施访问控制，根据数据包头中源/目的 IP 地址、源/目的端口号、协议类型等域的信息实施过滤。过滤防火墙的优点是速度快、透明性好；但缺乏用户日志(Log)和审计(Audit)信息，缺乏用户认证机制，安全性较差。

电路层网关在传输层实施访问策略，与应用层网关类似，但它是在内外网络主机间建立一个虚拟电路进行通信，相当于在防火墙上直接开了个口子进行传输。不能象应用层防火墙那样严密地控制应用层的信息。

代理防火墙工作在应用层，对每个提供的服务构造一个代理(Proxy)负责实施所需的安全策略，可以实施用户认证、详细的日志和审计跟踪功能及对具体协议的过

滤(如阻塞 Java 或 JavaScript)。代理防火墙具有更高的灵活性和安全性,但可能影响网络性能,可能对用户不透明。

目前比较有名的防火墙产品有 TIS 公司的 Gauntlet Internet Firewall, Microsoft 的 Microsoft Proxy Server, Netscape 的 Netscape Proxy Server, Cisco 的 PIX 系列, Checkpoint 的 Firewall - 1, Digital 的 Alta Vista Firewall, Raptor System 的 Eagle Firewall 等。

三、防火墙新技术

各种类型的防火墙各有其优缺点,当前的防火墙产品往往结合了过滤层网关、电路层网关和应用层网关的功能,形成一个混合网关,而以下的一些新技术的支持可以在防火墙上提供更高的灵活性和安全性。

1. 动态包过滤(Dynamic Packet Filtering)

传统的包过滤基于单个 IP 包包头中的源/目的 IP 地址、源/目的端口号、协议类型等判断是否转发或丢弃此包。动态包过滤还可以与数据流相适应,基于 TCP 连接和通信过程中的状态变化及上下文内容,建立临时会话状态表来控制访问。如 TIS 公司提出的 Stateful filtering,有人认为它是另一种防火墙,但它其实就是一种动态过滤,还是属于包过滤防火墙;Cisco PIX 防火墙对数据包也是进行动态过滤,其核心是基于适应性安全算法(ASA)的保护方案,ASA 跟踪每个信息包的源地址、目的地址、TCP 序列数、端口号和其他 TCP 标志,将这些信息存入表格,所有进入的信息包与其比较,只有存在适当的连接来承认信息包的合法性时,此信息包才能通过防火墙。动态过滤比静态过滤更安全。

2. 内核级透明代理(Transparent Proxy on Kernel Level)

克服操作系统(OS)本身因系统庞大而可能存在的安全缺陷,采用最小内核技术,OS 内核仅是一个"安全骨架",去除了 OS 中所有不必要的服务和其他子系统,关闭了 IP forwarding 功能,可加入对 IPSec、IP(v6)等的支持以提供加密的 IP 通信,对提供的服务也仅给以最小特权,并使提供的服务相互独立,以提供防火墙的安全基石。由于在内核级实现了代理服务,代理可以做到协议透明和应用透明;可采用包截取方法获取数据包,作出授权校验后,决定转发或丢弃,此过程对用户可以是透明的。

3. 增强的用户认证机制(Advanced User Authentication Mechanism)

克服可重用口令在公共网上明文传输的缺点,对用户远程访问实施强认证,并配合多防火墙的互操作能力,提供分布式跨域认证的能力。强认证系统有 SecurID、Enigma Logic、S/key 等。可采用基于第三方的认证服务器,基于用户(组)、地址(组)、服务类型、时间等要求认证。一次性口令系统是一种较好的认证机制,其优点是口令不重用,既不在客户端也不在服务器端存储秘密口令,但在分布式认证方面有一定的缺陷。

4. 多防火墙之间的互操作性和对 VPN 的支持(Interoperability between Multiple Firewalls & VPN Support)

由于防火墙的安全机制是基于对内部网中所有用户和系统信任的基础之上,缺乏对来自内部攻击的防范能力,可以将内部网络划分成多个子网,用防火墙来分隔连接各子网。为在多个防火墙上实现统一的安全策略,防火墙支持对多个代理服务的单点同步管理和远程管理。防火墙支持较远距离的通过公用网传送数据的多个网络的 VPN(Virtual Private Network)能力,提供加密措施、防止信息泄漏。VPN 支持公开和秘密密钥,使用 X.500 目录和 X.509 证书,自动进行数据加/解密和密钥,提供在 Internet 上建立加密通道安全透明地进行数据通信。

5. 内容类型感知和策略感知能力(Content Type - aware & Policy - awareness)

代理按其对传输内容的感知能力可分为电路层(Circuit Layer:只处理包头域)、数据包感知(Traffic - aware:对数据包中某些字节可进行一些特殊处理)、命令感知(Command - aware:理解支持的一些命令)、内容类型感知(Content Type - aware:不仅理解命令,还理解传输内容的一般格式)和策略感知(Policy - aware:不仅知道内容类型,还带有一定的人工智能,可以根据本地策略对传输内容进行解码和处理)五种。具有内容类型和策略感知能力的防火墙不仅理解传输类型,还理解本地策略,可根据本地策略自适应地进行处理。如在防火墙上进行病毒扫描和过滤、黄色信息过滤、对 FTP 下载的自抽取文档过滤以检测隐藏在多媒体数据中的非法命令等。

6. 内部网络信息隐藏(Internal Information Hide)

使用网络地址翻译(NAT:Network Address Translator)技术可使内部地址信息实现隐藏,对公开的信息服务器可以采用静态映射,对内部主机采用多对多的地址映射或多对一的地址映射(通常为防火墙主机的外部地址)。在防火墙上内外部域名和帐号等之间建立映射关系而保护内部信息。

7. 智能型日志、审计和实时告警(Intelligent Log&Audit and Real-time Alert)

日志系统具有综合性数据记录功能和自动分类检索能力;审计系统提供对防火墙的完整性校验,具有追踪多次连接行为的能力;告警系统利用日志审计结果,监测网络探测、端口扫描等,通过智能性地推理,自动实时触发E-mail、窗口、呼叫、打印等进行告警,在极端情况下可自动中断服务或关闭系统。

8. 其他

为消除防火墙作为单失败点的缺陷,可采用双机备份运行技术;支持 SNMP 管理;支持 RealAudio、RealVideo、Cu-SeeMe、Streamwork 等多媒体应用;提供 QoS(Quality of Service)能力;专用防火墙为提高吞吐量可引入智能 I/O 处理高带宽应用;结合安全代理和高速传输介质如 ATM 上的快速处理能力,可适应性地控制、监测数据包重组以优化在交换数据时的安全检查,对高速应用数据流提供高度安全性控制;并且防火墙作为统一的安全策略的实现点,可提供对 Intranet 资源的监控,分析系统性能趋向,平衡服务器的负载,管理和计划使用网络带宽;及提供对其他安全协议的支持。

参考文献

[1] Scott Fuller, Kevin Pagan 著. Intranet 防火墙. 董春, 张红雨, 刘英杰译:电子工业出版社,1997

[2] Randall J. Atkinson. Toward a More Secure Internet. IEEE Computer. 1997,(1)

[3] RFC1636

[4] David Newman, Brent Melson. Can Firewalls Take the Heat?. Data Communication. 1995,(11)

[5] Rofe Oppliger. Internet Security: Firewalls and Beyond. Communications of the ACM. Vol 40 No 2. 1997,(2)

(来稿时间:1998 年 3 月)