网络攻击分类研究

重庆工商大学计算机科学与信息工程学院计算机科学与技术专业　周　炜

一、引言

在网络这个不断更新换代的世界里，网络中的安全漏洞无处不在。即便旧的安全漏洞补上了，新的安全漏洞又将不断涌现。网络攻击正是利用这些存在的漏洞和安全缺陷对系统和资源进行攻击。我对网络攻击的各类方式以及攻击者常使用的工具进行了一些研究，并且总结出了一些有效实用的应对策略。

二、网络攻击的原理和手法

1 口令入侵

所谓口令入侵是指使用某些合法用户的帐号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的帐号，然后再进行合法用户口令的破译。利用目标主机的 Finger 功能；利用目标主机的 X.500 服务；从电子邮件地址中收集；查看主机是否有习惯性的帐号；

2 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载。当您连接到因特网上时，这个程序就会通知攻击者，来报告您的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

3 WWW 的欺骗技术

在网上用户可以利用 IE 等浏览器进行各种各样的 WEB 站点的访问，然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

4 电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。攻击者可以使用一些邮件炸弹软件或 CGI 程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被撑爆而无法使用。电子邮件攻击主要表现为两种方式：

(1)是电子邮件轰炸和电子邮件"滚雪球"，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被"炸"，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；

(2)是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序。

5 通过一个节点来攻击其他节点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。

6 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。

7 利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。它们可以非法地取得用户电脑的超级用户级权利，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以进行对方桌面抓图、取得密码等操作。

8 安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bugs）。其中一些是操作系统或应用软件本身具有的。如缓冲区溢出攻击。由于很多系统在不检查程序与缓冲之间变化的情况，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。

9 端口扫描攻击

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有：Connect()扫描。Fragmentation 扫描。

三、攻击者常用的攻击工具

1 攻击工具

如 WinNuke 通过发送 OOB 漏洞导致系统蓝屏；Bonk 通过发送大量伪造的 UDP 数据包导致系统重启；TearDrop 通过发送重叠的 IP 碎片导致系统的 TCP/IP 栈崩溃；WinArp 通过发特殊数据包在对方机器上产生大量的窗口；Land 通过发送大量伪造源 IP 的基于 SYN 的 TCP 请求导致系统重启动；FluShot 通过发送特定 IP 包导致系统凝固；Bloo 通过发送大量的 ICMP 数据包导致系统变慢甚至凝固；PIMP 通过 IGMP 漏洞导致系统蓝屏甚至重新启动；Jolt 通过大量伪造的 ICMP 和 UDP 导致系统变的非常慢甚至重新启动。

2 木马程序

(1)BO2000(BackOrifice)：它是功能最全的 TCP／IP 构架的攻击工具，可以搜集信息，执行系统命令，重新设置机器，重新定向网络的客户端／服务器应用程序。

简易低频信号测试系统设计

重庆工商大学计算机与信息工程学院04级测控技术与仪器　胡　浩

摘　要:介绍了基于单片机控制的低频信号测试系统,用于测量信号源为0~100kHz的低频信号。文中简要阐述了系统的软硬件设计以及LCD液晶显示。

关键字:低频信号　单片机　液晶显示

通过简易低频信号测试仪的设计、安装和调试,熟悉运用51单片机来开发设计仪器的过程;学会选择合适的集成块电路合理搭建最小单片机系统;通过对电路元器件的安装和布线,熟悉对单片机外围电路的制作;掌握程序和硬件电路的调试方法。

一、基本原理

1 频率的测量

频率的测量实际上就是在1S时间内对信号进行计数,计数值就是信号频率。用单片机设计频率计通常采用两种办法:

1)单片机外部使用计数器对脉冲信号进行计数,计数值再由单片机读取;

2)使用单片机自带的计数器对输入脉冲进行计数,或者测量信号的周期。

2 结构框图

---

(2)"冰河":冰河是一个国产木马程序,具有简单的中文使用界面,且只有少数流行的反病毒、防火墙才能查出冰河的存在。

(3)NetSpy:可以运行于Windows95/98/NT/2000等多种平台上,它是一个基于TCP/IP的简单的文件传送软件,但实际上你可以将它看作一个没有权限控制的增强型FTP服务器。通过它,攻击者可以神不知鬼不觉地下载和上传目标机器上的任意文件,并可以执行一些特殊的操作。

(4)Glacier:该程序可以自动跟踪目标计算机的屏幕变化、获取目标计算机登录口令及各种密码类信息、获取目标计算机系统信息、限制目标计算机系统功能、任意操作目标计算机文件及目录、远程关机、发送信息等多种监控功能。类似于BO2000。

(5)Keyboard:Windows系统是一个以消息循环(MessageLoop)为基础的操作系统。系统的核心区保留了一定的字节作为键盘输入的缓冲区,其数据结构形式是队列。键盘幽灵正是通过直接访问这一队列,使键盘上输入你的电子邮箱、代理的账号、密码Password(显示在屏幕上的是星号)得以记录,一切涉及以星号形式显示出来的密码窗口的所有符号都会被记录下来,并在系统根目录下生成一文件名为KG.DAT的隐含文件。

(6)ExeBind:这个程序可以将指定的攻击程序捆绑到任何一个广为传播的热门软件上,使宿主程序执行时,寄生程序也在后台被执行,且支持多重捆绑。实际上是通过多次分割文件,多次从父进程中调用子进程来实现的。

四、网络攻击应对策略

在对网络攻击进行上述分析与识别的基础上,我们应当认真制定有针对性的策略。明确安全对象,设置强有力的安全保障体系。有的放矢,在网络中层层设防,发挥网络的每层作用,使每一层都成为一道关卡,从而让攻击者无隙可钻、无计可使。还必须做到未雨稠缪,预防为主,将重要的数据备份并时刻注意系统运行状况。以下是针对众多令人担心的网络安全问题,提出的几点建议:

1 提高安全意识

不要随意打开来历不明的电子邮件及文件,不要随便运行不太了解的人给你的程序,比如"特洛伊"类黑客程序就需要骗你运行。尽量避免从Internet下载不知名的软件、游戏程序。密码设置尽可能使用字母数字混排,单纯的英文或者数字很容易穷举。)及时下载安装系统补丁程序。不随便运行黑客程序,不少这类程序运行时会发出你的个人信息。在支持HTML的BBS上,如发现提交警告,先看源代码,很可能是骗取密码的陷阱。使用防毒、防黑等防火墙软件。

2 设置代理服务器,隐藏自己的IP地址。

保护自己的IP地址是很重要的。事实上,即便你的机器上被安装了木马程序,若没有你的IP地址,攻击者也是没有办法的,而保护IP地址的最好方法就是设置代理服务器。代理服务器能起到外部网络申请访问内部网络的中间转接作用,其功能类似于一个数据转发器,它主要控制哪些用户能访问哪些服务类型。

3 将防毒、防黑当成日常例性工作,定时更新防毒组件,将防毒软件保持在常驻状态,以彻底防毒。

参考文献

[1]程秉辉:John Hawke 编著《黑客任务实战(攻略篇)》[M]北京希望电子出版社 2002

[2]程秉辉:John Hawke 编著《黑客任务实战(防护篇)》[M]北京希望电子出版社 2002