网络安全 – 程序攻击

逻辑炸弹攻击

植入后门

蠕虫&特洛伊木马攻击

木马的实现技术

逻辑炸弹攻击 – 定义

一种隐藏于计算机系统中以某种方式触发后，对计算机系统硬件、软件或数据进行恶意破坏的程序代码

触发方式

- 时间触发、特定操作触发、满足某一条件的触发等

计算机病毒攻击

生物病毒

- **一种微小的基因代码段—DNA或RNA，它能掌管活细胞机构，并采用欺骗性手段生成成千上万的原病毒的复制品**

计算机病毒（第13章 网络病毒防治）

- **一段附着在其它程序上的、可以自我繁殖的程序代码**

逻辑炸弹攻击 – 特征

隐蔽性：逻辑炸弹一般都比较短小，容易附着在系统或文件上而不容易察觉，也可能被恶意隐藏在一些常用工具软件代码中

攻击性：逻辑炸弹都具有攻击性，一旦被激发，或是干扰屏幕显示，或降低电脑运行速度，或是删除程序，破坏数据

逻辑炸弹没有“传染性”

如何投放?

江民硬盘逻辑炸弹

症状：不能进入系统，软盘、光盘不能引导进入

原因：硬盘锁死，应为改变了硬盘分区表

- **读取完分区表才能进入系统，如果分区是循环的?**

后门 – 定义

后门是计算机入侵者攻击网上其它计算机成功后为方便下次进入这台被攻击计算机而采取的一些欺骗手段和程序

目的

- **再次进入、不被发现**
- **健壮性**

后门 – 攻击方法

获取尽可能多的用户口令，并不会被管理员察觉或查封

更改配置

- **例如：rhosts**

替换程序（包括源代码，函数库，内核）

- **要点：时间、校验和**

开设新的服务，定时开启服务

后门的植入 - 寻找可用作后门的系统漏洞

登录程序后门

- 其身份验证过程可能存在漏洞，使用这类后门可以方便地登录系统，并且不容易被发现

网络服务后门

- 一些系统服务程序或应用服务程序中存在着漏洞，如系统服务Telnet, Ftp, E-mail, Rlogin 等和应用服务IRC, OICQ 等

系统库后门

- 系统库用于函数的重用而减少代码长度
- 利用系统库来安装后门可以做 到很隐秘，成功率也很高

内核后门

- 内核是操作系统工作的核心，但内核模块的处理过程存在一些漏洞

后门的植入 - 植入木马等后门代理程序

远程管理型木马可以提供很好的后门服务

木马的安装主要是利用系统操作者不好的使用习惯和薄弱的安全意识潜入系统

- 如操作人员随意上网抓资料或太信任电子邮件送来的文件等。

目前，大多数的特洛伊木马都可用作后门代理程序

还有其他的吗？

后门的隐藏技术

应用级隐藏是常规的隐藏方法，通过修改、捆绑或替代系统合法的应用程序来实现隐藏。早期的后门一般是在应用级上实现隐藏

内核级隐藏一种是指在支持LKMs(Loadable Kernel Modules) 的操作系统上实现隐藏; 另一种是通过系统库来实现隐藏

内核级隐藏是比较难于检测的，能避过目前绝大多数后门扫描工 具、查杀病毒软件和入侵检测系统的检测

后门 - 远程监控技术

对计算机的监视包括对主机的鼠标、键盘以及屏幕显示甚至网络通讯流量流向等的监视，也包括对对方计算机系统信息（包括磁盘信息、操作系统信息及硬件信息）的搜集

远程控制则是攻击者控制目标机，按照自己的意愿在被攻击计算机上运行程序或者关闭对方的功能，包括控制对方的鼠标、键盘、操作系统，在对方计算机上启动服务，或者关闭对方计算机等

蠕虫

技术等级相当高，利用提供网络服务的软件漏洞来达到在远程计算机上的自我复制

步骤

1. 入侵计算机，传入网络
2. 获得用户账号
3. 找出提供直接访问而无需身份鉴定的主机，实现自我复制

- 还有其他方法?

特洛伊木马

简称木马，英文名为Trojan horse

计算机领域的“特洛伊木马(Trojan)”，是指附着在应用程序中或者单独存在的一些恶意程序

利用网络远程响应网络另一端的控制程序的控制命令，实现对感染木马程序的计算机的控制，或者窃取感染木马程序的计算机上的机密资料。

UNIX到Window的两个阶段

病毒、蠕虫、木马的区别

普通病毒需要传播受感染的驻留文件来进行复制

蠕虫不使用驻留文件即可在系统之间进行自我复制

木马表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。

- 它是具有欺骗性的文件(宣称是良性的，但事实上是恶意的)，是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

特洛伊木马 - 工作原理

木马程序一般利用TCP/IP协议，采用C/S结构，分为客户端和服务器端两个部分

服务器端程序运行于被攻击的计算机上，而客户端程序在控制者的计算机上运行客户端程序，可以同时向很多服务端程序发送命令以控制这些计算机

客户端程序一般提供友好的操作界面，以便于用户的操作，其功能可能很多

特洛伊木马 – 按攻击方式分类

远程访问型木马

密码发送型木马

键盘记录型木马

毁坏型木马

FTP型木马

特洛伊木马 – 按传输方式分类

主动型木马

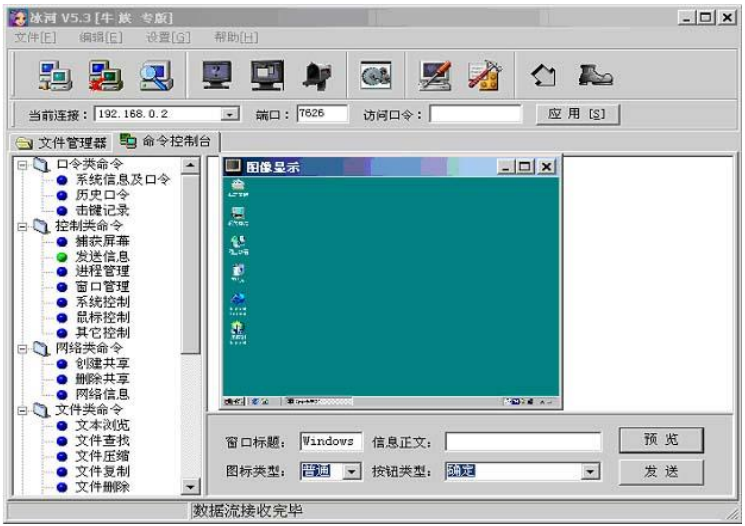
反弹型木马

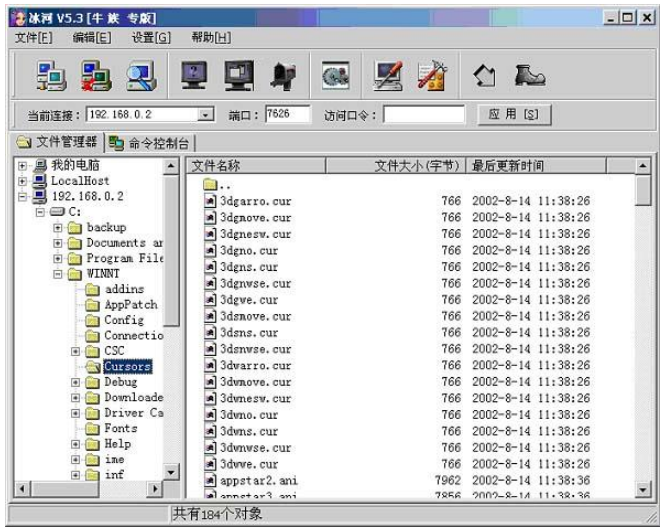
嵌入式木马

特洛伊木马 – 主动型木马

攻击者客户端可扫描到被攻击者

- 文件浏览器
- 屏幕监视
- 键盘鼠标控制

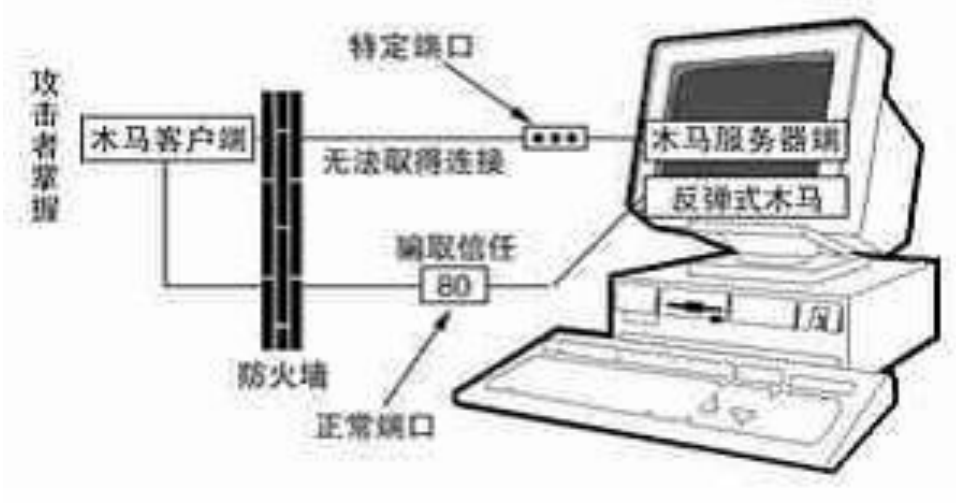




特洛伊木马 - 反弹型木马

技术动机?

它利用防火墙对内部发起的连接请求无条件信任的特点，假冒是系统的合法网络请求，与木马的客户端建立连接，从而达到对被攻击计算机控制的目的



特洛伊木马 - 网络神偷

远程文件访问，而不是远程控制

反弹端口

HTTP 隧道

服务器端上线通知功能

通讯加密

嵌入式木马

不管是主动式还是反弹式木马，都需要建立新的Socket，建立客户端和被控制服务端的通信

嵌入式木马隐藏于常用网络程序中，利用这类程序转发木马命令

宿主程序关闭，木马程序就不起作用

后门 VS 木马

后门是一个允许攻击者绕过系统中常规安全控制机制的程序，他按照攻击者自己的意图提供通道。

后门的重点在于为攻击者提供进入目标计算机的通道

如果一个程序仅仅提供远程访问，那么它只是一个后门

如果攻击者将这些后门伪装成某些其他良性程序，那么那就变成真正的特洛伊木马

如何防御木马、后门

培养良好的安全意识和习惯

使用网络防火墙封锁与端口的连接

- **仅允许最少数量的端口通信通过防火墙**

经常利用端口扫描器扫描主机或端口，查看工具查找本地端口监听程序。

- **Nmap，Xscan，NC，TcpView，IceSword……**

木马的实现技术

自动启动技术

- 第一次需要用户启动，之后在启动系统时候自动加载

隐藏技术

- 与普通程序的最大区别
- DLL用于木马的技术
  - 替换DLL
  - 动态嵌入

远程控制技术

Rootkit 看不到的一定不存在吗?

恶意程序通常会在系统留下痕迹。

- **文件**
- **进程**
- **端口号**
- **注册表启动键值**
- **……**

看不到就一定不存在吗?

- **RootKit**

Rootkit定义

什么是 Rootkit [此处只讨论基于Windows平台的]

- Rootkit与普通木马、后门以及病毒的区别

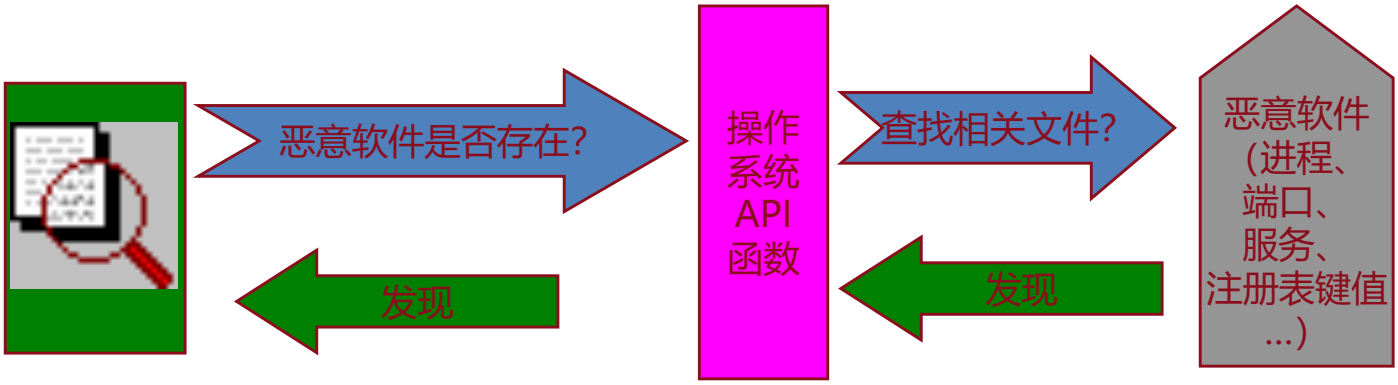
Rootkit宗旨：隐蔽

- 通信隐蔽、自启动项隐藏、文件隐藏、进程/模块隐藏、
- 注册表隐藏、服务隐藏、端口隐藏 etc.

研究内核级后门Rootkit技术的必要性

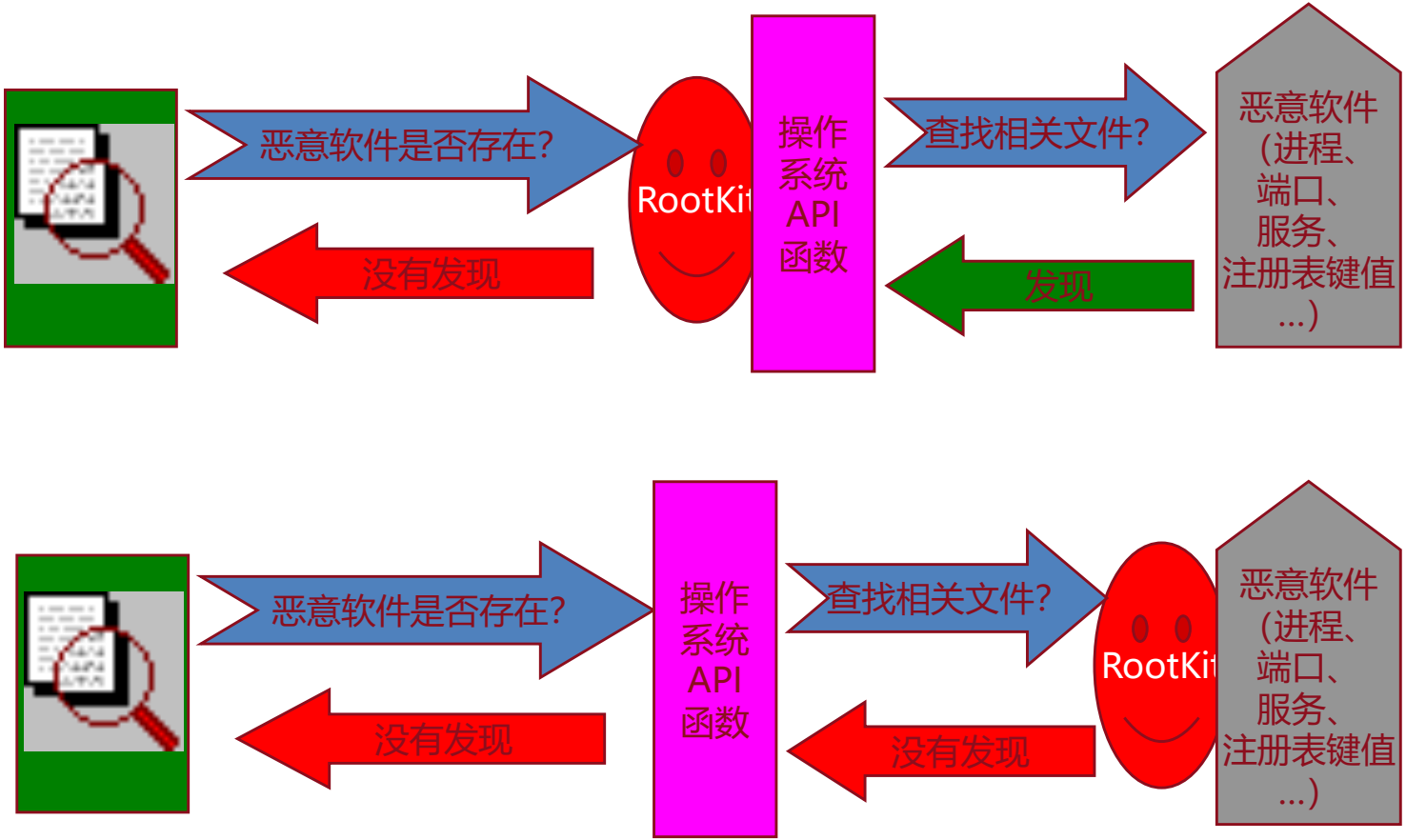
- 事物两面性；信息战、情报战 ……

正常的系统查询过程



它们的操作指令全部依赖于内核授权的功能，我们能看到的进程其实是内核“看到”并通过相关接口指令反馈到应用程序的。

RootKit入侵之后的系统查询过程



Rootkit特性

Rootkit实质是一种“越权执行”的应用程序，它设法让自己达到和内核一样的运行级别，甚至进入内核空间，这样它就拥有了和内核一样的访问权限，因而可以对内核指令进行修改，最常见的是修改内核枚举进程的API，让它们返回的数据始终“遗漏”Rootkit自身进程的信息，一般的进程工具自然就“看”不到Rootkit了。

更高级的Rootkit还篡改更多API，这样，用户就看不到进程（进程API被拦截），看不到文件（文件读写API被拦截），看不到被打开的端口（网络组件Sock API被拦截），更拦截不到相关的网络数据包（网络组件NDIS API被拦截）了

幸好网络设备的数据指示不受内核控制，否则如果内核变得不可信任了，依赖它运行的程序还能信任吗?

木马的发展

第一代，是最原始的木马程序。主要是简单的密码窃取，通过电子邮件发送信息等，具备了木马最基本的功能。

第二代，在技术上有了很大的进步，冰河是中国木马的典型代表之一。

第三代，主要改进在数据传递技术方面，出现了ICMP等类型的木马，利用畸形报文传递数据，增加了杀毒软件查杀识别的难度。

第四代 在进程隐藏方面有了很大改动，采用了内核插入式的嵌入方式，利用远程插入线程技术，嵌入DLL线程。

第五代，驱动级木马多数都使用了大量的Rootkit技术来达到在深度隐藏的效果

第六代，随着身份认证和杀毒软件主动防御的兴起，蠕虫技术类型木马逐渐开始系统化。

木马的种类

网络游戏木马

网银木马

即时通讯软件木马

- 发送消息型、盗号型、传播自身型

网页点击类木马

下载类木马

代理类木马