

# 第6章 网络威胁

许海燕



# 主要内容

- ◆ 6.1 概述
- ◆ 6.2 计算机病毒
- ◆ 6.3 网络入侵
- ◆ 6.4 诱骗类威胁



## 6.1 概述

- ◆ **威胁**：用威力逼迫恫吓使人屈服。
- ◆ **网络威胁**：是网络安全受到威胁、存在着危险。
- ◆ 随着互联网的不断发展，网络安全威胁也呈现了一种新的趋势，
  - 最初的病毒，比如“CIH”、“大麻”等传统病毒
  - 逐渐发展为包括特洛伊木马、后门程序、流氓软件、间谍软件、广告软件、网络钓鱼、垃圾邮件等等，
  - 目前的网络威胁往往是集多种特征于一体的混合型威胁。

# 网络威胁的三个阶段

- ◆ 第一阶段（1998年以前）网络威胁主要来源于传统的计算机病毒，其特征是通过媒介复制进行传染，以攻击破坏个人电脑为目的；
- ◆ 第二阶段（大致在1998年以后）网络威胁主要以蠕虫病毒和黑客攻击为主，其表现为蠕虫病毒通过网络大面积爆发及黑客攻击一些服务网站；
- ◆ 第三阶段（2005年以来）网络威胁多样化，多数以偷窃资料、控制利用主机等手段谋取经济利益为目的。



# 网络威胁分类

## ◆ 从攻击发起者的角度来看，

- 一类是主动攻击型威胁，如网络监听和黑客攻击等，这些威胁都是对方人为通过网络通信连接进行的；
- 另一类就是被动型威胁，一般是用户通过某种途径访问了不当的信息而受到的攻击。

## ◆ 依据攻击手段及破坏方式进行分类

- 第一类是以传统病毒、蠕虫、木马等为代表的计算机病毒；
- 第二类是以黑客攻击为代表的网络入侵；
- 第三类以间谍软件、广告软件、网络钓鱼软件为代表的欺骗类威胁。



# 主要内容

- ◆ 6.1 概述
- ◆ 6.2 **计算机病毒**
- ◆ 6.3 网络入侵
- ◆ 6.4 诱骗类威胁



## 6.2 计算机病毒

### ◆ 6.2.1 病毒概述

- 1949年约翰·冯·诺依曼《自我繁衍的自动机理论》中从理论上论证了当今计算机病毒的存在论。
- 20世纪60年代初，美国贝尔实验室的三位程序员编写了一个名为“磁芯大战”的游戏
- 1983年，美国南加州大学的弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，第一次验证了计算机病毒的存在。
- 1984年弗雷德·科恩《计算机病毒：原理和实验》。
- 1986年Brain病毒，世界上流行的第一个病毒。
- 1988年罗伯特·塔潘·莫里斯（美国前国家安全局首席科学家罗伯特·莫里斯的儿子）编写Morris蠕虫。

# 计算机病毒定义

## ◆ 《中华人民共和国计算机信息系统安全保护条例》中明确定义：

- 病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。





## ◆ 计算机病毒特征

- (1) 非授权性
- (2) 寄生性
- (3) 传染性
- (4) 潜伏性
- (5) 破坏性
- (6) 触发性

## ◆ 计算机病毒发展新的趋势

无国界  
多样化  
破坏性更强  
智能化  
更加隐蔽化

## ◆ 计算机病毒可以根据其工作原理和传播方式划分成

传统病毒

蠕虫病毒

木马



## 6.2.2 传统病毒

### ◆ 传统病毒的代表

- 巴基斯坦智囊 ( Brain )、大麻、磁盘杀手 ( DISK KILLER )、CIH

### ◆ 传统病毒一般有三个主要模块组成，包括启动模块、传染模块和破坏模块。

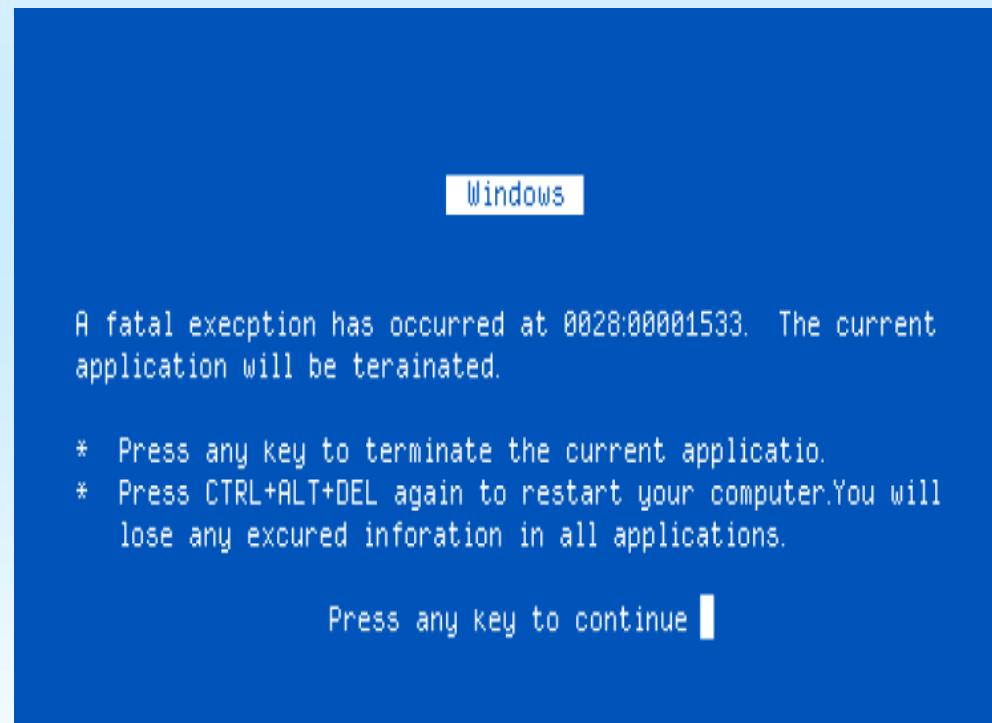
### ◆ CIH

- 感染Windows95/98环境下PE格式的EXE文件 ( 第一例 )
- 病毒发作时直接攻击和破坏计算机硬件系统。
- 该病毒通过文件复制进行传播。
- 计算机开机后，运行了带病毒的文件，其病毒就驻留在Windows核心内存里
- 组成：初始化驻留模块、传染模块和破坏模块。



# CIH

- 当系统的时钟走到了4月26日这一天，中了CIH病毒的计算机将受到巨大的打击。病毒开始发作时，出现“蓝屏”现象，并且提示当前应用被终止，系统需要重新启动



# CIH

- 当计算机被重新启动后，用户会发现自己计算机硬盘上的数据被全部删除了，甚至某些计算机使用者主板上Flash ROM中的BIOS数据被清除

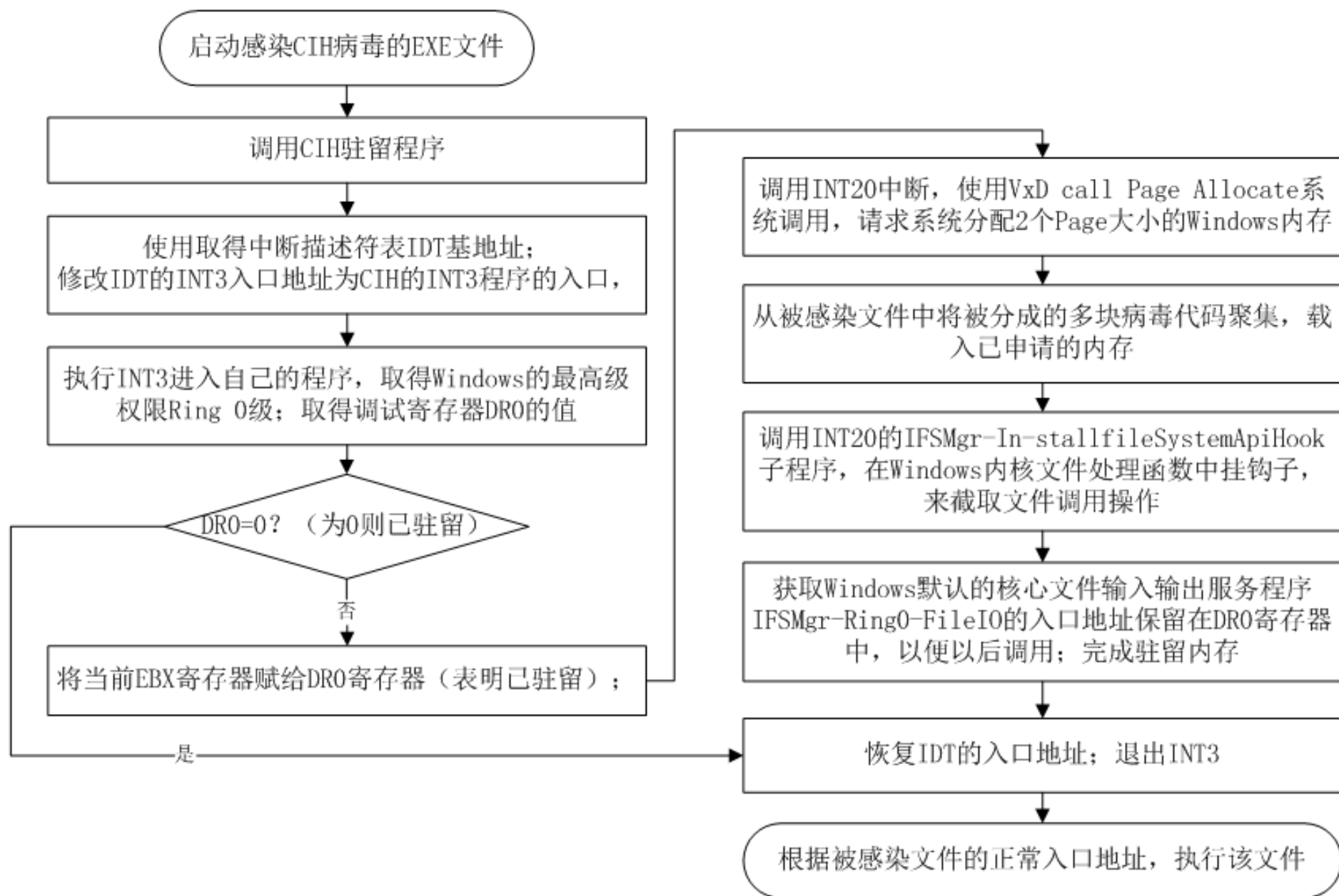
```
Diskette Drive A : 1.44M,3.5"      Display Type      : EGA/VGA
Diskette Drive A : None            Serial Port(s)    : 3F8 2F8
Pri. Master Disk : CDROM,ATA 33     Parallel Port(s) : 370
Pri. Master Disk : LBA,ATA 33,40022MB DOR at Row(s)      : 0
Pri. Master Disk : CD-RW,ATA 33     DRAM ECC Mode    : Disabled
Pri. Master Disk : None

Pri. Slave Disk  HDD  S.M.A.R.T. capability .... Disabled

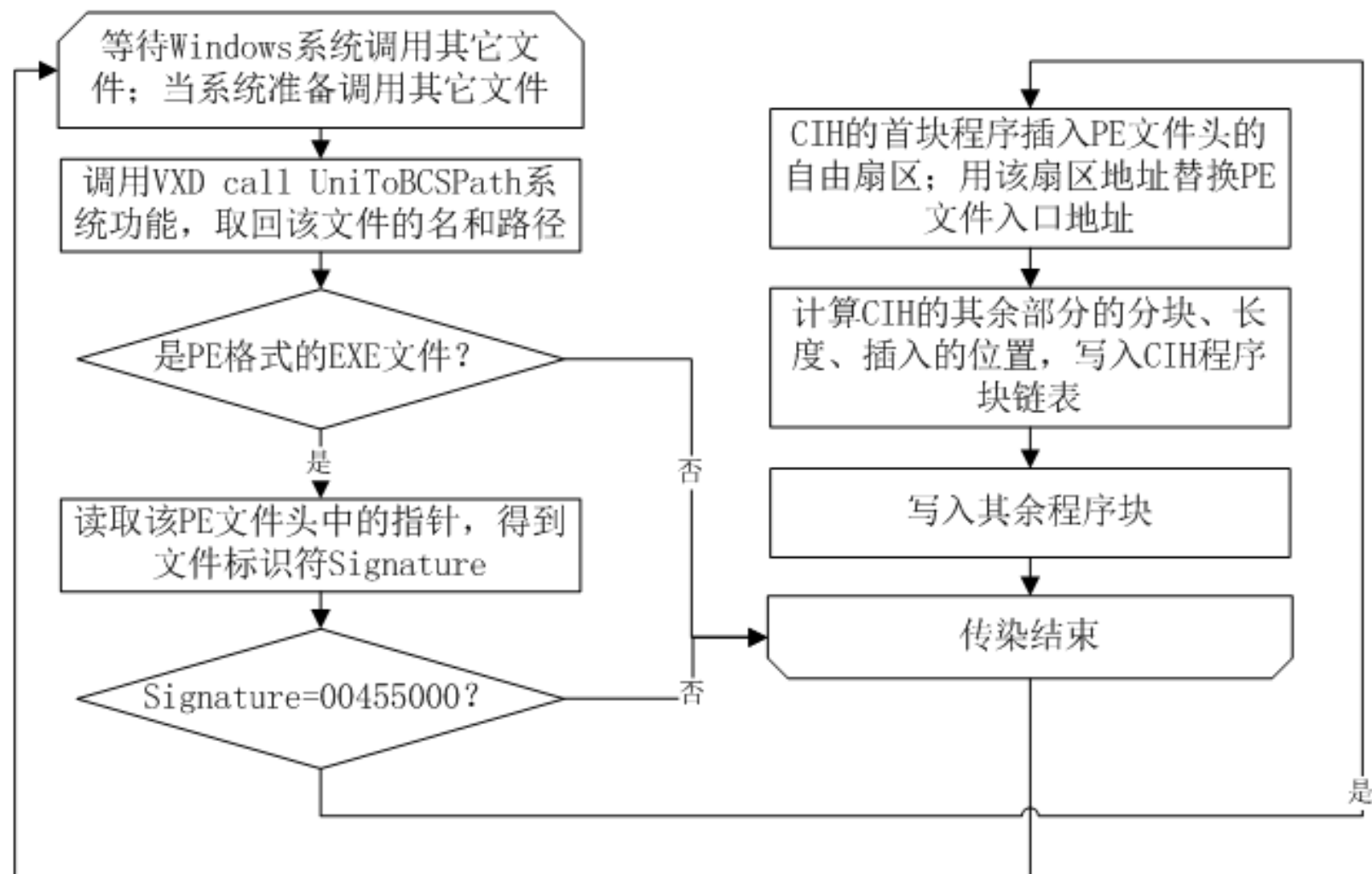
Verifying DMI Pool Data .....
Boot Form CD :
Boot Form CD :
DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER
-
```



## 驻留初始化模块



## 传染模块



## 破坏模块

从系统CMOS中取出当前日期DATA

DATA=26/4?

是

向BIOS的引导区写入乱码;  
向硬盘写入乱码覆盖硬盘;

否

结束



## 6.2.3 蠕虫病毒

### ◆ 蠕虫与传统病毒的区别：

- 传统病毒是需要的寄生的，通过感染其它文件进行传播。
- 蠕虫病毒一般不需要寄生在宿主文件中，传播途径主要包括局域网内的共享文件夹、电子邮件、网络中的恶意网页和大量存在着漏洞的服务器等。
- 可以说蠕虫病毒是以计算机为载体，以网络为攻击对象。

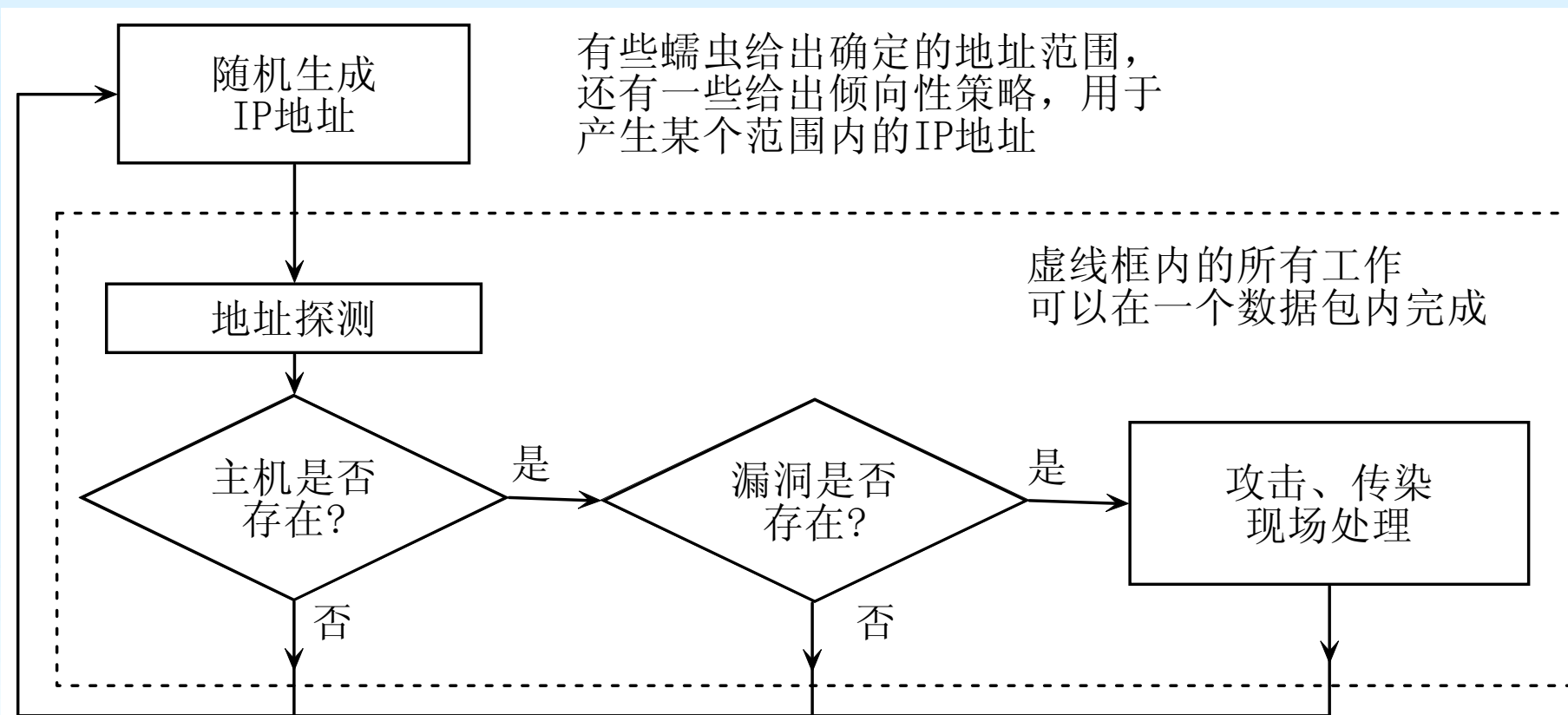
### ◆ 蠕虫病毒能够利用漏洞，分为软件漏洞和人为缺陷

- 软件漏洞主要指程序员由于习惯不规范、错误理解或想当然，在软件中留下存在安全隐患的代码
- 人为缺陷主要指的是计算机用户的疏忽，这就是所谓的社会工程学（Social Engineering）问题。



# 蠕虫的工作方式与扫描策略

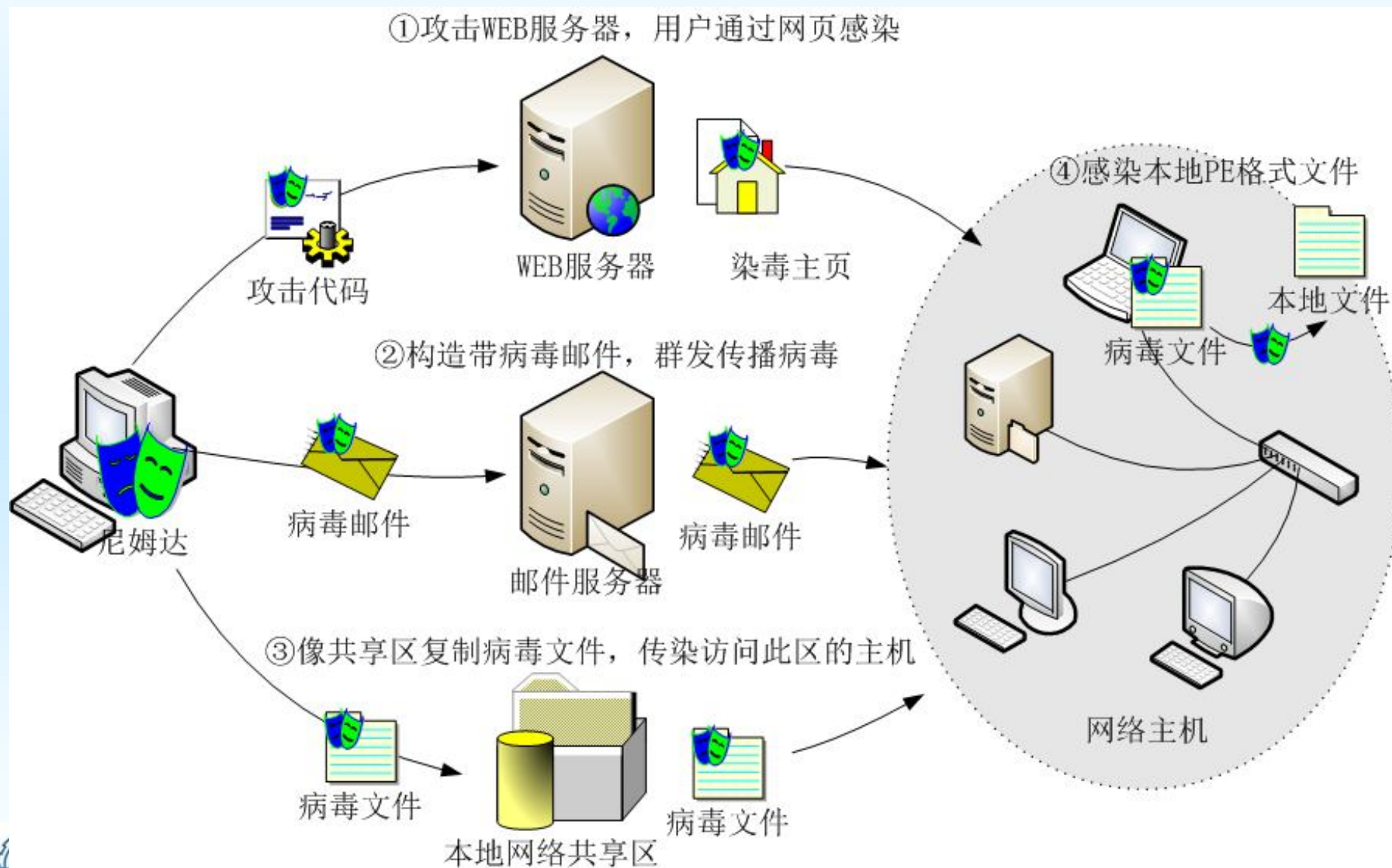
## ◆ 蠕虫的工作方式一般是“扫描→攻击→复制”



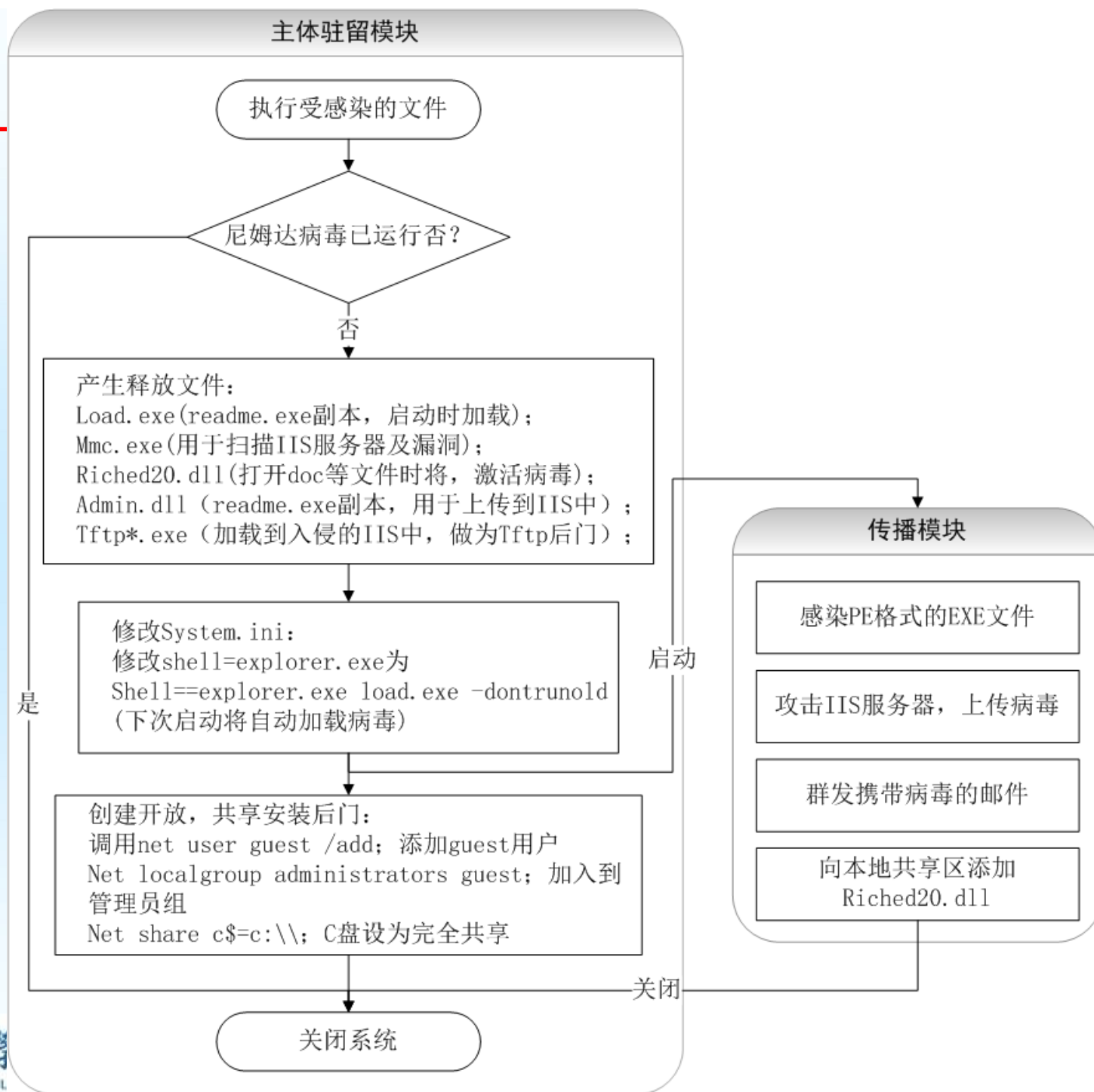
# 尼姆达蠕虫Worms.Nimda

- ◆ 2001年9月18日尼姆达病毒在全球蔓延，它能够通过各种传播渠道进行传播，传染性极强，同时破坏力也极大。
  - 尼姆达病毒是一个精心设计的蠕虫病毒，其结构复杂堪称近年来之最。
  - 尼姆达病毒激活后，使用其副本替换系统文件；将系统的各驱动器设为开放共享，降低系统安全性；创建Guest账号并将其加入到管理员组中，安装Guest用户后门。
  - 由于尼姆达病毒通过网络大量传播，产生大量异常的网络流量和大量的垃圾邮件，网络性能势必受到严重影响。

# Nimda 传播途径



# 尼姆达病毒程序



## 6.2.4 木马

- ◆ 木马病毒，“木马计”，伪装潜伏的网络病毒。
  - 1986年的PC-Write木马是世界上第一个计算机木马
  - 木马是有隐藏性的、传播性的可被用来进行恶意行为的程序，因此，也被看作是一种计算机病毒。
  - 木马一般不会直接对电脑产生危害，以控制电脑为目的，当然电脑一旦被木马所控制，后果不堪设想。
- ◆ 木马的传播（种木马或植入木马）方式
  - 主要通过电子邮件附件、被挂载木马的网页以及捆绑了木马程序的应用软件。
  - 木马被下载安装后完成修改注册表、驻留内存、安装后门程序、设置开机加载等，甚至能够使杀毒程序、个人防火墙等防范软件失效。

# 木马病毒程序组成

## 木马病毒分类

- (1) 盗号类木马
- (2) 网页点击类木马
- (3) 下载类木马
- (4) 代理类木马

## 控制端程序(客户端)

是黑客用来控制远程计算机中的木马的程序；

## 木马程序（服务器端）

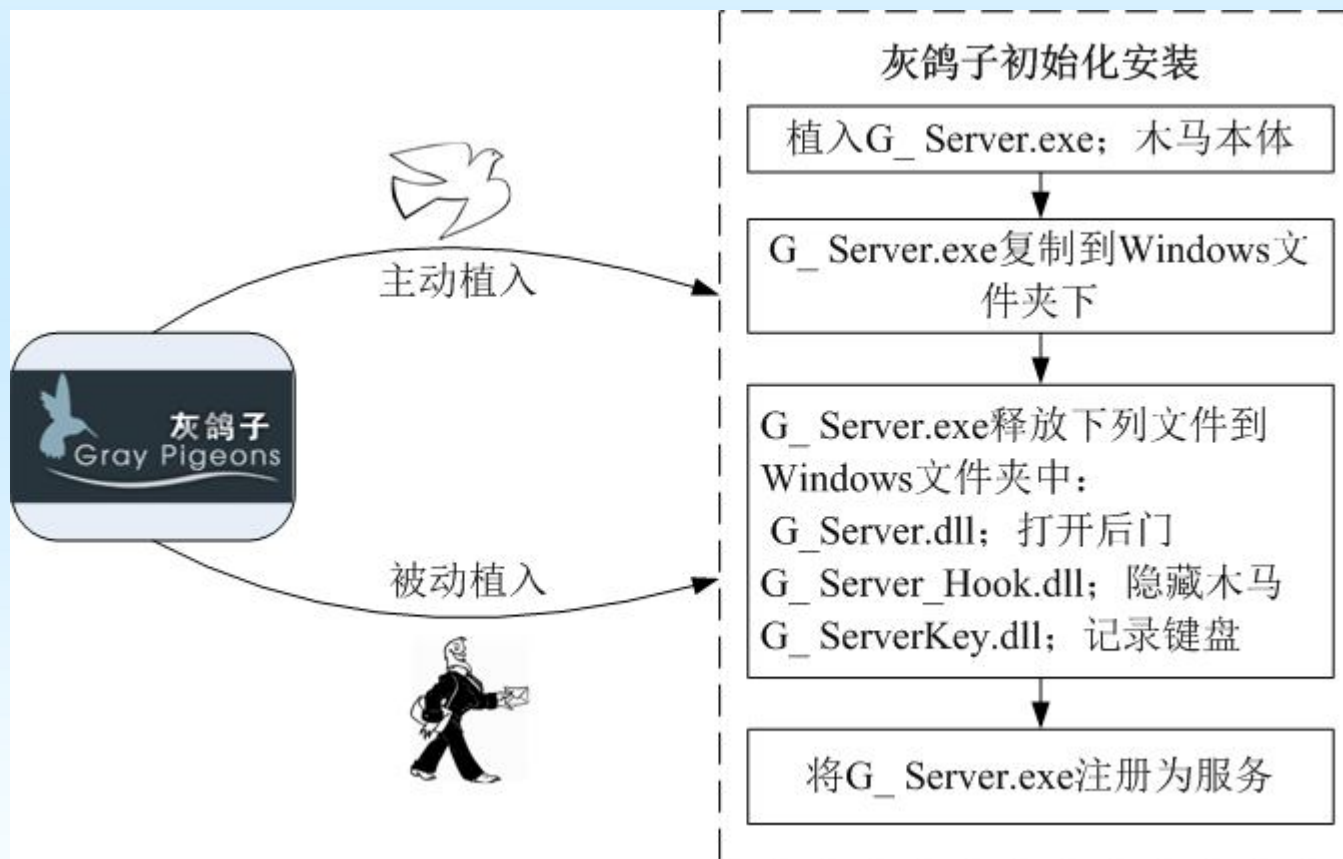
是木马病毒的核心，是潜入被感染的计算机内部、获取其操作权限的程序；

## 木马配置程序，

通过修改木马名称、图标等来伪装隐藏木马程序，并配置端口号、回送地址等信息确定反馈信息的传输路径。

# 灰鸽子的植入方法

- ◆ 被动植入是指植入过程必须依赖受害用户的手工操作；
- ◆ 主动植入是将灰鸽子程序通过程序自动安装到目标系统。



# 灰鸽子的隐藏技术

- ◆ 隐藏文件
- ◆ 隐藏进程
- ◆ 隐藏通讯

- 通讯端口复用技术是指将自己的通讯直接绑定到正常用户进程的端口，接收数据后，根据包格式判断是不是自己的，如果是它的，自己处理，否则通过127.0.0.1的地址交给真正的服务器应用进行处理。
- 反弹端口技术是指木马程序启动后主动连接客户，为了隐蔽起见，控制端的被动端口一般设置为80端口。对内部网络到外部网络的访问请求，防火墙一般不进行过于严格的检查，加之其连接请求有可能伪造成对外部资源的正常访问，因此可以通过防火墙。





# 客户端程序

## ◆ 定制生成服务器端程序。

- 首先利用客户端程序配置生成一个服务器端程序文件，服务器端文件的名称默认为G\_Server.exe，然后开始在网络中传播植入这个程序。

## ◆ 控制远程的服务器端。

- 当木马植入成功后，系统启动时木马就会加载运行，然后反弹端口技术主动连接客户控制端。

## ◆ 客户控制端程序的功能：

- 对远程计算机文件管理
- 远程控制命令
- 捕获屏幕，实时控制
- 注册表模拟器

## 6.2.5 病毒防治

- ◆ 病毒防治技术略滞后于病毒技术
- ◆ 对于大多数计算机用户来说，防治病毒首先需要选择一个有效的防病毒产品，并及时进行产品升级。

# 反病毒软件的构成

## 应用程序

- 进行病毒扫描、提供反病毒软件与用户的交互接口。

## 引擎

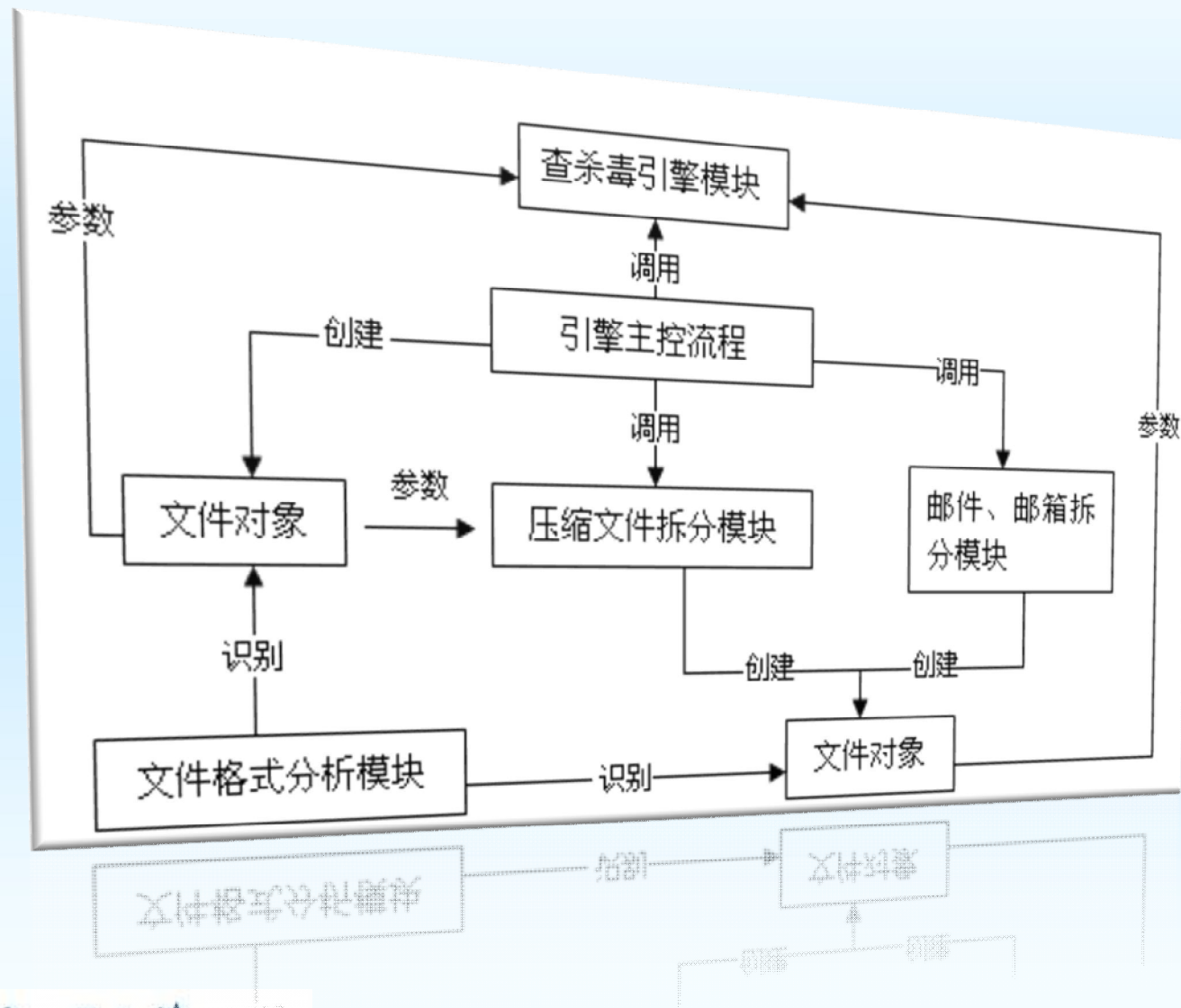
- 对应用程序传入的扫描对象进行格式分析和病毒扫描，返回结果进行相应的处理。
- 引擎本身还负责病毒库的加载、管理、遍历及卸载。

## 病毒库

- 病毒数据库
- 黑白名单



# 引擎的体系构架



# 反病毒引擎的技术特征

邮件、  
压缩包  
拆分

虚拟与  
真实的  
脱壳

木马  
特征

利用可  
行引擎  
特征提  
取

病毒解  
码和杀  
的相关

内存扫  
描和存  
在监控

未知病  
毒虚拟  
执行

未知脚  
本病毒  
特征判  
定

行为  
判定



# 1、反病毒引擎（杀毒引擎）特点

杀毒引擎就是一套判断特定程序行为是否为病毒程序（包括可疑的）的技术机制。一个完整的技术引擎遵守如下的行为过程：

- 1.非自身程序行为的程序行为捕获。引擎前端。
- 2.基于引擎机制的规则判断。这个环节被叫做杀毒软件引擎工作的核心层。



# 1、反病毒引擎（杀毒引擎）特点（续）

3.引擎与病毒库的交互作用。杀毒引擎与要将非自身程序行为过程转化为杀毒软件自身可识别的行为标识符（包括静态代码等），然后与病毒库中所存贮的行为信息进行对应，并作出相应处理。

- ✓当前的杀毒软件对大量病毒的识别都是在这个阶段完成的。
- ✓因此一个足够庞大的病毒库往往能够弥补杀毒软件引擎的不足之处。
- ✓如果在核心层阶段就可以结束并清除病毒程序，那么杀毒软件的工作速度将会大幅提升。
- ✓当前我们没有足够聪明的杀毒引擎来完成这个过程，这就是为什么有病毒库的原因。





## 2、反病毒引擎（杀毒引擎）类型

1. Dr.web(大蜘蛛):是俄罗斯官方和军队采用的产品。它的技术以俄罗斯国家科学院为后盾。除了该公司自己的产品外，采用该引擎的品牌还有“韩国驱逐舰”和“德国小红伞”。它从来不把二进制病毒和不能发做的木马列入病毒库，但对付变种病毒和木马绝对强悍，可以干掉加密XTA算法的病毒。
2. Kaspersky (卡巴斯基)：来自俄罗斯的世界著名杀毒软件——反病毒引擎和病毒库，一直以其严谨的结构和快速的反应速度为业界所称道——杀毒强悍、果断、彻底是其一大特点。正是因为如此，它连年获得国际杀毒软件排名“亚军”和诸多奖项的殊荣，目前世界上用卡巴斯基引擎的品牌非常多。



## 2、反病毒引擎（杀毒引擎）类型（续）

- 3、Norton(诺顿)：防止侦测方面做得不是很好，所以有时被病毒破坏。但其隔离机制还是很完善的。
- 4、McAfee(麦咖啡)：来自美国的著名杀毒软件。收购所罗门公司——所罗门的引擎。全球最畅销的杀毒软件之一(世界排名第六)。它具有自动监视系统，会常驻在System Tray。
- 5、Panda(熊猫卫士)：——在欧洲占有很大市场份额，查杀速度绝对一流。占用内存较大。

### 3、反病毒引擎采用的技术

- ◆ 计算机病毒防治技术主要包括:

- 检测、清除、预防和免疫。

- ✓ 检测和清除是根治病毒的有力手段,
    - ✓ 预防和免疫也是保证计算机系统安全的重要措施



# 病毒检测

1) 病毒检测方法主要包括：特征代码法、校验和法、行为监测法以及软件模拟法等。

## 1. 特征代码法

- 特征代码查毒就是检查文件中是否含有病毒数据库中的病毒特征代码。

## 2. 校验和法

- 对正常状态下的重要文件进行计算，取得其校验和，以后定期检查这些文件的校验和与原来保存的校验和是否一致。



# 病毒检测

## 3. 行为监测法

- 利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。当一个可疑程序运行时，监视其行为，如果发现了病毒行为，立即报警。

## 4. 软件模拟法

- 软件模拟法是为了对付多态型病毒。软件模拟法是通过模拟病毒的执行环境，为其构造虚拟机，然后在虚拟机中执行病毒引擎解码程序，安全地将多态型病毒解开并还原其本来面目，再加以扫描。软件模拟法的优点是可识别未知病毒、病毒定位准确、误报率低；缺点是检测速度受到一定影响、消耗系统资源较高。

# 病毒清除

- ◆ 将染毒文件的病毒代码部分摘除，将其恢复为可用的正常文件
- ◆ 病毒的清除可用专用的软件杀毒或手工进行
- ◆ 隔离是指在发现病毒后，无法确认清除动作会带来什么后果，又不想直接删除文件，故采取监视病毒并阻止病毒运行的方法。
  - 某类病毒清除失败、删除失败、隔离失败，对个人用户来讲，格式化硬盘、重建系统可能就是最后的有效选择。



# 免疫

## ◆ 计算机病毒免疫

- 提高计算机对计算机病毒的抵抗力，从而达到防止病毒侵害的目的
- 一是提高计算机系统的健壮性，二是给计算机注射“病毒疫苗”。
- 提高系统健壮性的主要途径包括以下内容：
  - ✓ 及时升级操作系统，保证系统安装最新的补丁；
  - ✓ 安装防病毒软件，及时升级病毒定义文件和防病毒引擎；
  - ✓ 定期扫描系统和磁盘文件；
  - ✓ 打开个人防火墙；
  - ✓ 使用软盘或U盘写保护
  - ✓ 重要的数据信息写入只读光盘；

# 计算机病毒的免疫

- ◆ 计算机病毒免疫的原理：根据病毒的签名来实现。这是由于一些病毒在感染其他文件时会先判断是否已经感染，即检测欲感染的文件是否存在**病毒签名**，如有则不再感染。
- ◆ 因此可以人为地在“健康程序”中进行病毒签名，起到免疫效果



# 主要内容

- ◆ 6.1 概述
- ◆ 6.2 计算机病毒
- ◆ 6.3 网络入侵
- ◆ 6.4 诱骗类威胁





## 6.3 网络入侵

- ◆ 1980年，James P Anderson首次提出了“入侵”的概念，
  - ✓ “入侵”是指在非授权的情况下，试图存取信息、处理信息或破坏系统，以使系统不可靠或不可用的故意行为。
  - ✓ 网络入侵一般是指具有熟练编写、调试和使用计算机程序的技巧的人，利用这些技巧来获得非法或未授权的网络或文件的访问，进入内部网的行为。
  - ✓ 对信息的非授权访问一般被称为破解cracking。

## 6.3.1 黑客入侵的一般流程

隐藏自身



预攻击探测



收集信息,如**OS**类型,提供的服务端口

发现漏洞,采取攻击行为



破解口令文件,或利用缓存溢出漏洞

获得攻击目标的控制权系统



获得系统帐号权限,并提升为**root,administrator**权限

安装系统后门



方便以后使用

继续渗透网络,直至获取机密数据



以此主机为跳板,寻找其它主机的漏洞

消灭踪迹

消除所有入侵脚印,以免被管理员发觉



## 6.3.2 攻击的技术与方法

现在网络上的攻击行为很多，这里只列出了典型的几种攻击行为。

- 1 预攻击探测
- 2 密码破解攻击
- 3 拒绝服务攻击
- 4 欺骗攻击
- 5 利用型攻击

# 1 预攻击探测

- ◆ 预攻击探测技术主要可以分为**Ping扫描、操作系统识别扫描、端口扫描以及漏洞扫描**（ Vulnerability Scan ）等。
  - Ping扫描用于发现攻击目标；
  - 操作系统识别扫描就是对目标主机运行的操作系统进行识别；
  - 端口扫描用于查看攻击目标处于监听或运行状态的服务；
  - 漏洞扫描就是扫描对方系统有什么漏洞可以利用。
  - 目前主流的扫描工具包括流光、Nmap、Nessus、SSS(Shadow Security Scanner)等都实现了这些技术。
- ◆ 这些技术既可以作为安全管理员检验安全措施是否有效的方法，也会被黑客利用作为发动攻击的探测手段。下面介绍主要的预攻击探测技术。

# 1 预攻击探测

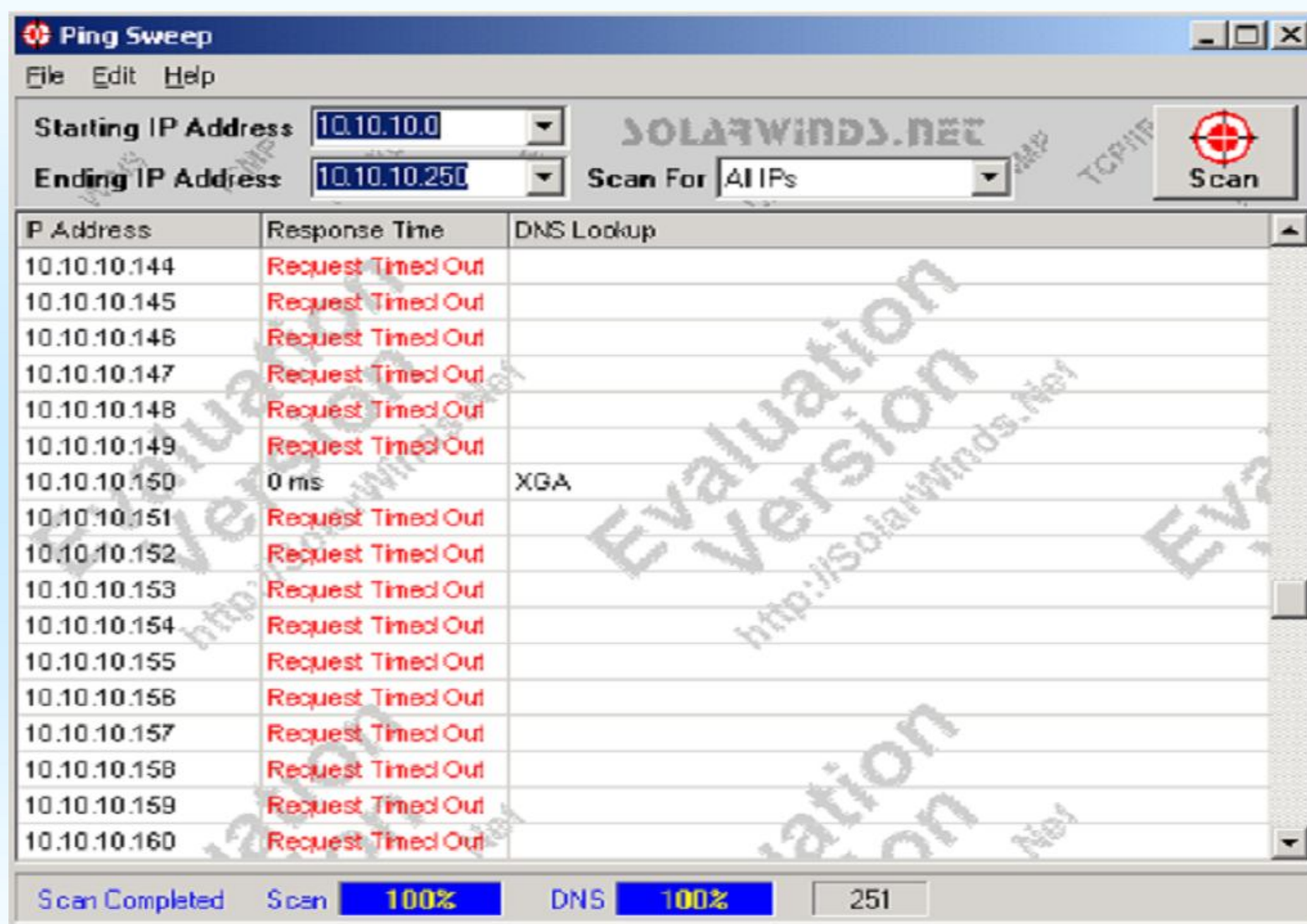
## ◆ Ping 扫描

使用Ping命令来进行扫描是平时最常用的方法。Ping扫描使用网络层的ICMP协议，用于搜寻对ICMP请求做出响应的计算机。

通常，Ping一个公司的Web服务器可帮助人们获得该公司所使用的IP地址范围。一旦得知了HTTP服务器的IP地址，可以使用Ping扫描工具Ping该子网的所有IP地址，这有助于得到该网络的地址图。

Windows 下的Ping工具很多，比如Pinger、Ping Sweep、WS\_Ping ProPack等。

# ping工具: Ping Sweep



# 网络结构发现

- ◆ 尽可能多的获取对方网络拓扑信息
- ◆ 分析对方网络结构
- ◆ 为进一步入侵做准备

# Traceroute命令

- ◆用于路由跟踪，判断从你的主机到目标主机经过哪些路由器、跳计数、响应时间等等
- ◆可以推测出网络物理布局
- ◆判断出响应较慢的节点和数据包在路由过程中的跳数
- ◆Traceroute或者使用极少被其它程序使用的高端UDP端口，或者使用PING数据包





# 1 预攻击探测

## ◆ 操作系统识别扫描

### ✧ 那么如何辨识一个操作系统

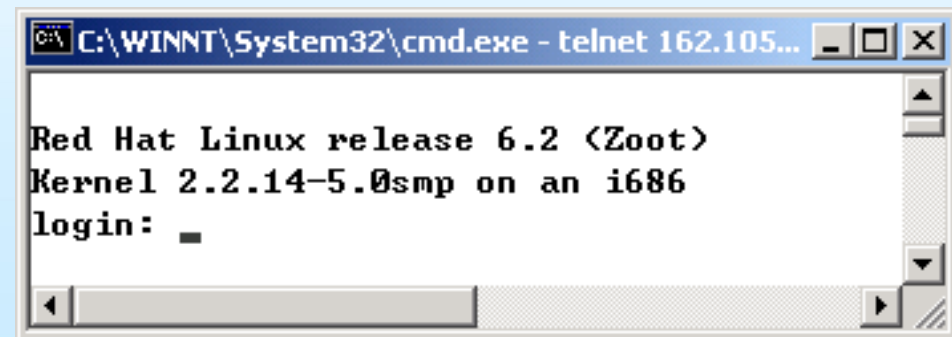
1. 一些端口服务的提示信息，例如，telnet、http、ftp等服务的提示信息
2. TCP/IP栈指纹
3. DNS泄漏出OS系统

# 端口服务提供的信息

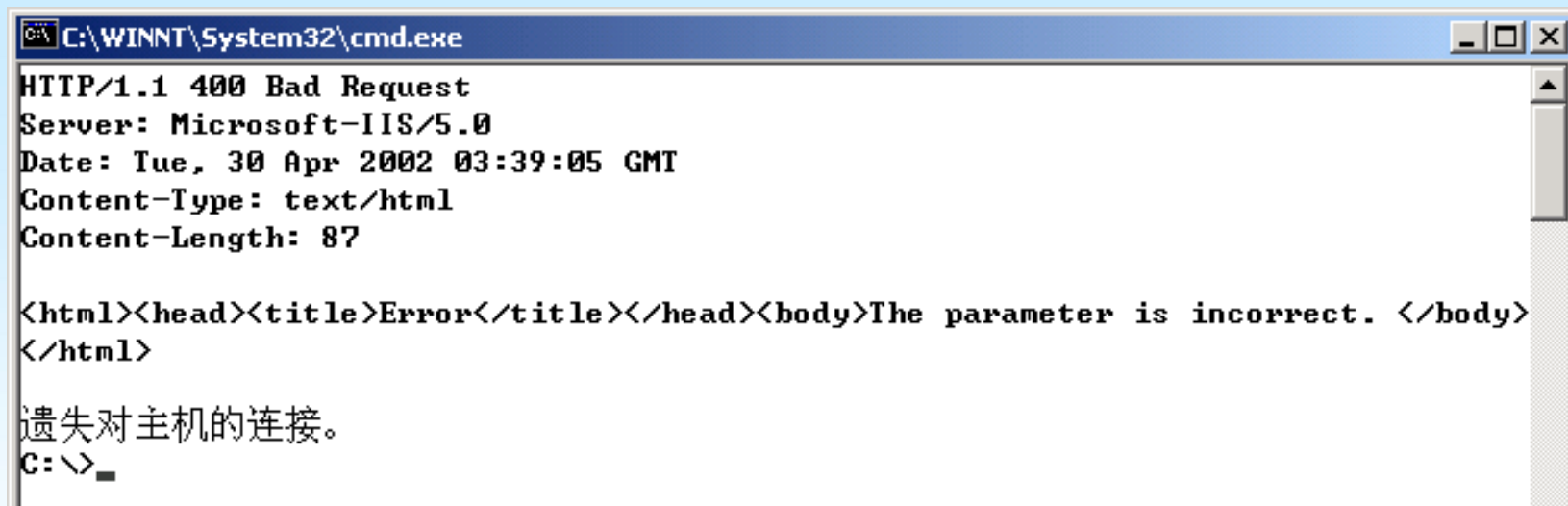
✧ Telnet服务

✧ Http服务

✧ Ftp服务



```
C:\WINNT\System32\cmd.exe - telnet 162.105...  
  
Red Hat Linux release 6.2 (Zoot)  
Kernel 2.2.14-5.0smp on an i686  
login: _
```



```
C:\WINNT\System32\cmd.exe  
HTTP/1.1 400 Bad Request  
Server: Microsoft-IIS/5.0  
Date: Tue, 30 Apr 2002 03:39:05 GMT  
Content-Type: text/html  
Content-Length: 87  
  
<html><head><title>Error</title></head><body>The parameter is incorrect. </body>  
</html>  
  
遗失对主机的连接。  
C:\>_
```



## ◆ 栈指纹技术

- ✧ 寻找不同操作系统之间在处理网络数据包上的差异，并且把足够的差异组合起来，以便精确地识别出一个系统的OS版本
  - 原因：不同的厂家在编写自己操作系统时，TCP/IP协议虽然是统一的，但对TCP/IP协议栈没有做统一的规定，厂家可以按自己的要求来编写TCP/IP协议栈，从而造成了操作系统之间协议栈的不同。因此可以通过分析协议栈的不同来区分不同的操作系统，只要建立起协议栈与操作系统对应的数据库，就可以准确地识别操作系统。目前来说，用这种技术识别操作系统是最准确，也是最科学的。因此也被称为识别操作系统的“指纹技术”。当然，识别的能力与准确性，就要看各软件的数据库建立情况了。

# 主动栈指纹识别方法

## ✧ 常用的手段

- ✓ 给一个开放的端口发送FIN包，有些操作系统有回应，有的没有回应
- ✓ 对于非正常数据包的反应
  - 比如，发送一个包含未定义TCP标记的数据包
- ✓ 根据TCP连接的序列号风格
  - 寻找初始序列号之间的规律
- ✓ ACK值
  - 有些系统会发送回所确认的TCP分组的序列号，有些会发回序列号加1
- ✓ TCP初始化窗口
  - 有些操作系统会使用一些固定的窗口大小
- ✓ DF位(Don't Fragment bit )
  - 某些操作系统会设置IP头的DF位来改善性能

# 主动栈指纹识别方法(续)

## ✧ 分片处理方式

- ✓ 分片重叠的情况下，处理会不同：用后到的新数据覆盖先到的旧数据或者反之

## ✧ ICMP协议

### ✓ ICMP错误消息的限制

- 发送一批UDP包给高端关闭的端口，然后计算返回来的不可达错误消息

### ✓ ICMP端口不可达消息的大小

- 通常情况下送回IP头+8个字节，但是个别系统送回的数据更多一些

### ✓ ICMP回应消息中对于校验和的处理方法不同

### ✓ ICMP回应消息中，TOS域的值

## ✧ TCP选项(RFC793和更新的RFC1323)



# 1 预攻击探测

## ◆ 端口扫描

- 端口是主机与外部通信的途径，一个端口就是一个潜在的通信通道，也可能是一个入侵通道。对目标主机进行端口扫描，能得到许多有用的信息。

# 1 预攻击探测

◆ 成功的建立一个TCP连接的流程如下：

CLIENT → SYN //CLIENT向SERVER发送一个SYN数据报

SERVER → SYN|ACK //SERVER向CLIENT发送回一个SYN|ACK数据包

CLIENT → ACK //CLIENT再向SERVER发送一个ACK，建立连接成功

◆ 连接不成功的流程如下：

CLIENT → SYN //CLIENT向SERVER发送一个SYN数据报

SERVER → RST|ACK //SERVER向CLIENT发送回一个RST|ACK数据包

CLIENT → RST //CLIENT再向SERVER发送一个RST，表示连接不成功



## 3.4.1 预攻击探测

◆ 关闭一个TCP连接过程:

CLIENT → FIN //CLIENT向SERVER发送一个FIN数据报(通知SERVER关闭);

SERVER → ACK //SERVER向CLIENT发送回一个FIN的ACK数据包(确认);

SERVER → FIN //SERVER向CLIENT发送回一个FIN数据包(通知CLIENT关闭);

CLIENT → ACK //CLIENT再向SERVER发送一个FIN的ACK(确认)

。





# 端口扫描原理



首先C发送一个TCP包（SYN 请求）给S，其中标记SYN（同步序号）要打开。SYN请求指明了客户端希望连接的服务器端端口号和客户端的初始序列号 ISN。然后，服务器端发回应答，包含自己的SYN信息ISN和对C的SYN应答，应答时返回下一个希望得到的字节序号。最后，C 对从S 来的SYN进行应答，数据发送开始。

在一个TCP/IP实现中，一般遵循以下原则：

- 当一个SYN或者FIN数据包到达一个关闭的端口，TCP丢弃数据包同时发送一个RST数据包。
- 当一个RST数据包到达一个监听端口，RST被丢弃。
- 当一个RST数据包到达一个关闭的端口，RST被丢弃。
- 当一个包含ACK的数据包到达一个监听端口时，数据包被丢弃，同时发送一个RST数据包。
- 当一个SYN位关闭的数据包到达一个监听端口时，数据包被丢弃。
- 当一个SYN数据包到达一个监听端口时，正常的三阶段握手继续，回答一个SYN|ACK数据包。
- 当一个FIN数据包到达一个监听端口时，数据包被丢弃。

许多端口扫描技术都是基于以上原则来设计的

# nmap

- ✧ By Fyodor
  - ✓ 作者研究了诸多扫描器，每一种扫描器都有自己的优点，它把所有这些技术集成起来，写成了nmap
- ✧ 源码开放，C语言
- ✧ 两篇技术文档
  - ✓ The Art of Port Scanning
  - ✓ Remote OS detection via TCP/IP Stack FingerPrinting
- ✧ 除了扫描功能，更重要的是，可以识别操作系统，甚至是内核的版本

**nmap**

Tools Profile Help

Host: 172.29.142.10-30 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 172.29.142.10-30

Hosts Services

Host
172.29.142.30
172.29.142.26
172.29.142.10

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 172.29.142.10-30

**Host is up** (0.00s latency).  
Not shown: 997 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds

**MAC Address:** 00:E0:4C:83:E3:8D (Realtek Semiconductor)  
Device type: general purpose  
Running: Microsoft Windows XP|2003  
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003  
Network Distance: 1 hop  
**TCP Sequence Prediction: Difficulty=257** (Good luck!)  
**IP ID Sequence Generation: Incremental**  
Service Info: OS: Windows

**Host script results:**

**|\_ nbstat:**

| NetBIOS name: HHHJJJ, NetBIOS user: <unknown>, NetBIOS MAC: 00:e0:4c:83:e3:8d (Realtek Semiconductor)  
| Names  
|\_ HHHJJJ<20> Flags: <unique><active>  
|\_ smb2-enabled: Server doesn't support SMBv2 protocol  
| smb-os-discovery:  
| OS: Windows XP (Windows 2000 LAN Manager)  
| Name: WORKGROUP\HHHJJJ  
|\_ System time: 2011-03-24 10:46:50 UTC+8

**TRACEROUTE**

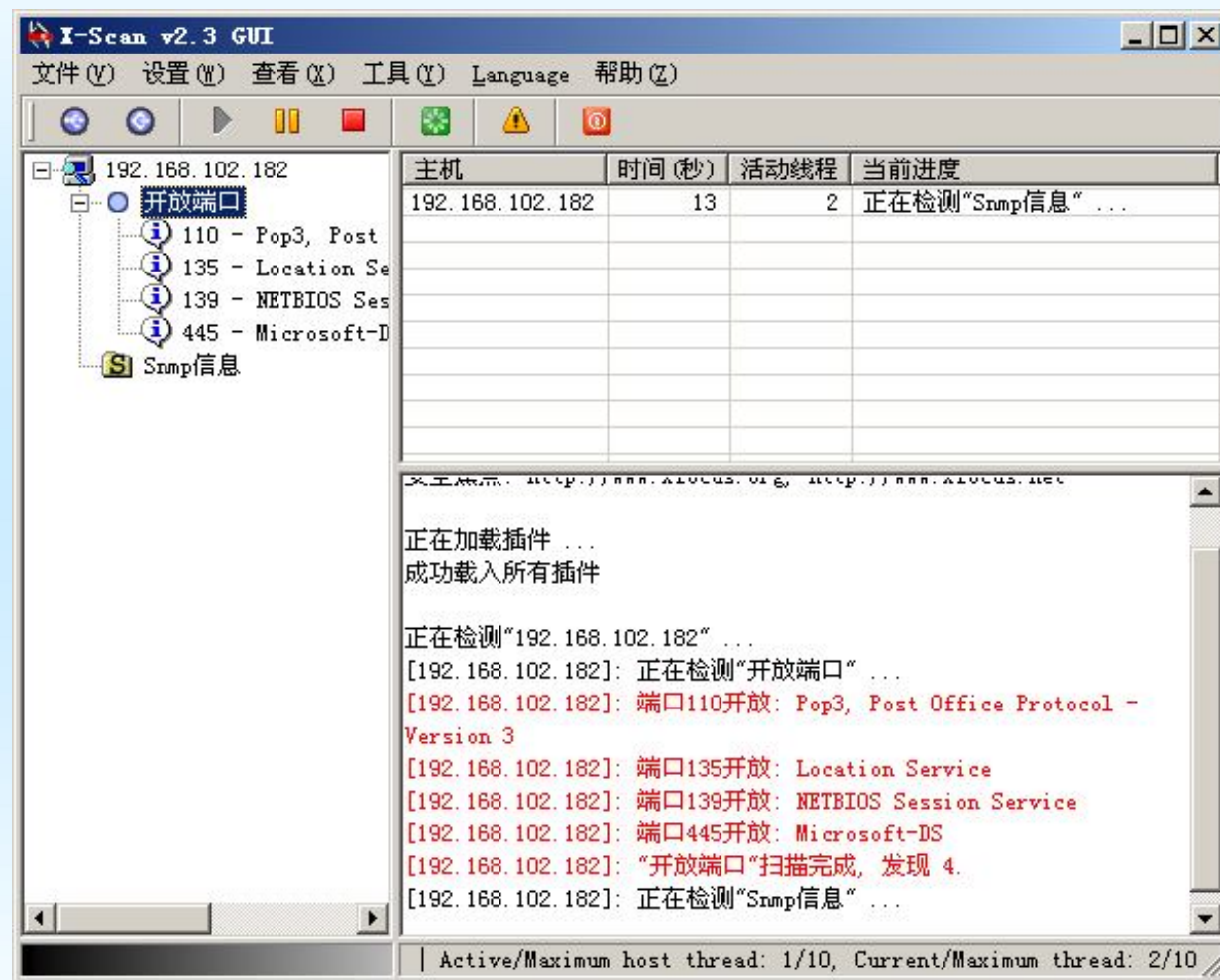
HOP	RTT	ADDRESS
1	0.00 ms	172.29.142.30

**Read data files from: D:\Program Files\Nmap**  
OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.  
Nmap done: 21 IP addresses (3 hosts up) scanned in 147.74 seconds  
Raw packets sent: 2149 (95.376KB) | Rcvd: 2035 (82.432KB)

Filter Hosts

Hosts shown Host Filter:

# X-scan



# 1 预攻击探测

## 漏洞扫描技术

### (1) 漏洞扫描技术的原理

- ◆ 漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：
  - 在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在；
  - 通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。

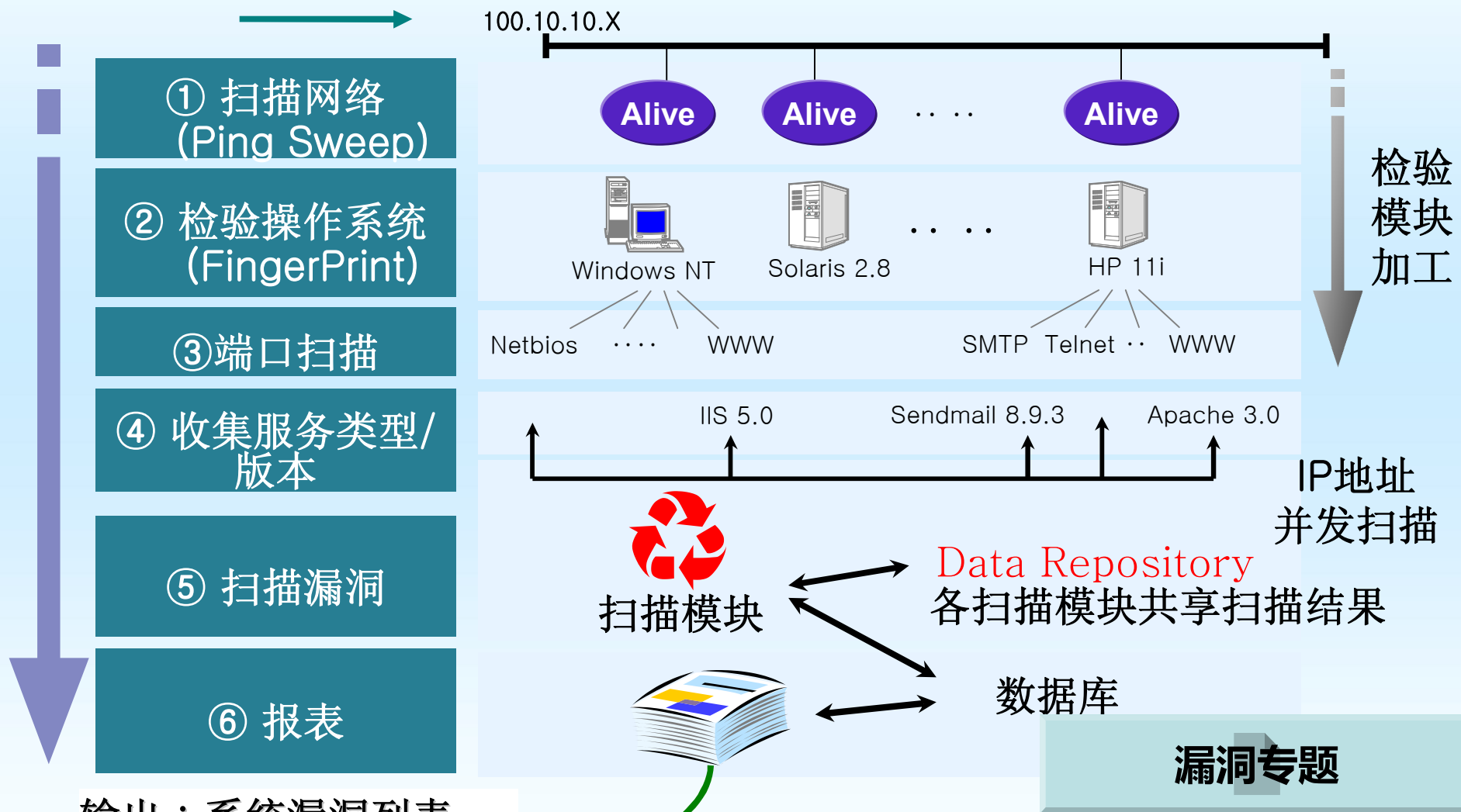
### (2) 漏洞扫描技术的分类和实现方法

- 基于网络系统漏洞库，漏洞扫描大体包括CGI漏洞扫描、POP3漏洞扫描、FTP漏洞扫描、SSH漏洞扫描、HTTP漏洞扫描等。这些漏洞扫描是基于漏洞库，将扫描结果与漏洞库相关数据匹配比较得到漏洞信息；
- 漏洞扫描还包括没有相应漏洞库的各种扫描，比如Unicode遍历目录漏洞探测、FTP弱势密码探测、OPENRelay邮件转发漏洞探测等，这些扫描通过使用插件（功能模块技术）进行模拟攻击，测试出目标主机的漏洞信息



# 漏洞检查方法

输入：扫描目标对象





## 2 密码破解攻击

### (1) 字典攻击

- ◆ 到目前为止，一个简单的字典攻击（Dictionary Attack）是闯入机器的最快方法。字典文件被装入破解应用程序（如L0phtCrack），它是根据由应用程序定位的用户账户运行的。因为大多数密码通常是简单的，所以运行字典攻击通常足以实现目的。

## 4.2 密码破解攻击

### 4 攻击的技术与方法

#### 2. 暴力攻击

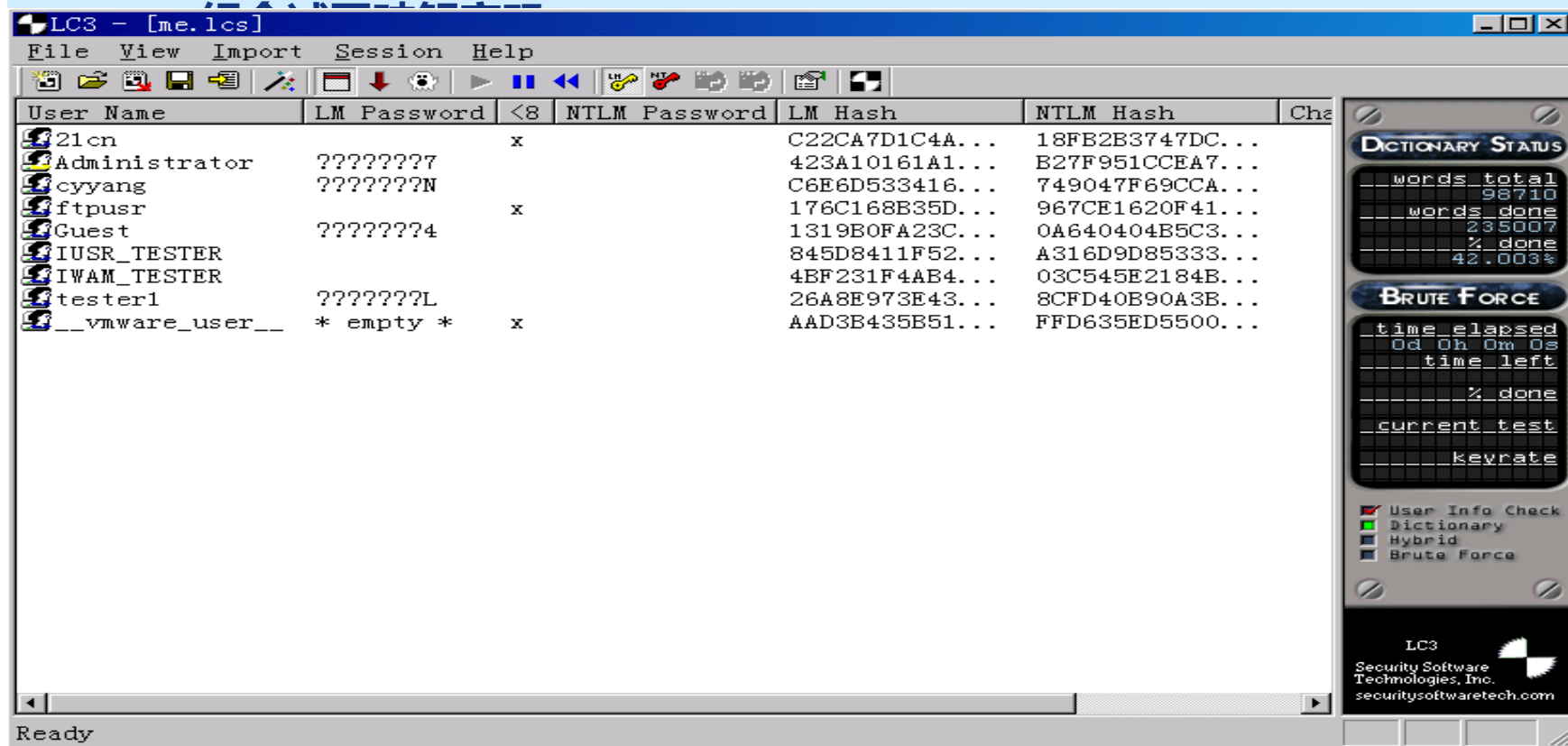
- ◆ 暴力攻击（**Brute Force Attack**）是最全面的攻击形式，虽然它通常需要很长的时间工作，这取决于密码的复杂程度。根据密码的复杂程度，某些暴力攻击可能花费一个星期的时间。工具：**L0phtcrack**。

## 2 密码破解攻击

### ◆ 常用的攻击工具：L0phtCrack和网络嗅探器。

#### (1) L0phtCrack

- ◆ 允许攻击者获取加密的Windows NT/2000 密码并将它们转换成纯文本的一种工具。NT/2000密码是密码散列格式，如果没有诸如L0phtCrack之类的工具就无法读取。它的工作方式是通过尝试每个可能的字母数字



# 3 拒绝服务攻击

## ◆ 拒绝服务攻击DoS (Denial of Service)

- DoS并不是某一种具体的攻击方式，而是攻击所表现出来的结果最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。

## ◆ 通常拒绝服务攻击可分为两种类型，

- 第一类攻击是利用网络协议的缺陷，通过发送一些非法数据包致使主机系统瘫痪；
- 第二类攻击是通过构造大量网络流量致使主机通讯或网络堵塞，使系统或网络不能响应正常的服务。



# Ping of Death

- ◆ TCP/IP的规范，一个包的长度最大为65536字节。
- ◆ 利用多个IP包分片的叠加能做到构造长度大于65536的IP数据包。
- ◆ 攻击者通过修改IP分片中的偏移量和段长度，使系统在接收到全部分段后重组报文时总的长度超过了65535字节。
- ◆ 一些操作系统在对这类超大数据包的处理上存在缺陷，当安装这些操作系统的主机收到了长度大于65536字节的数据包时，会出现内存分配错误，从而导致TCP/IP堆栈崩溃，造成死机。

# Tear drop

- ◆ IP数据包在网络传递时，数据包可能被分成多个更小的IP分片。
- ◆ 攻击者可以通过发送两个（或多个）IP分片数据包来实现Tear Drop攻击。
- ◆ 第一个IP分片包的偏移量为0，长度为N，第二个分片包的偏移量小于N，未超过第一个IP分片包的尾部，这就出现了偏移量重叠现象。
- ◆ 一些操作系统无法处理这些偏移量重叠的IP分片的重组，TCP/IP堆栈会出现内存分配错误，造成操作系统崩溃。

# Syn Flood

- ◆ 攻击者伪造TCP的连接请求，向被攻击的设备正在监听的端口发送大量的SYN连接请求报文；
- ◆ 被攻击的设备按照正常的处理过程，回应这个请求报文，同时为它分配了相应的资源。
- ◆ 攻击者不需要建立TCP连接，因此服务器根本不会接收到第三个ACK报文，现有分配的资源只能等待超时释放。
- ◆ 如果攻击者能够在超时时间到达之前发出足够多的攻击报文，被攻击的系统所预留所有TCP缓存将被耗尽。



# Smurf攻击

- ◆ Smurf攻击是以最初发动这种攻击的程序Smurf来命名的，这种攻击方法结合使用了IP地址欺骗和ICMP协议。
- ◆ 当一台网络主机通过广播地址将ICMP ECHO请求包发送给网络中的所有机器，网络主机接收到请求数据包后，会回应一个ICMP ECHO响应包，这样发送一个包会收到许多的响应包。
- ◆ Smurf构造并发送源地址为受害主机地址、目的地址为广播地址的ICMP ECHO请求包，收到请求包的网络主机同时响应并发送大量的信息给受害主机，致使受害主机崩溃。
- ◆ 如果Smurf攻击将回复地址设置成受害网络的广播地址，则网络中会充斥大量的ICMP ECHO响应包，导致网络阻塞。



# 电子邮件炸弹

## ◆ 实施电子邮件炸弹攻击的特殊程序称为Email Bomber。

- 邮箱容量是有限的，用户在短时间内收到成千上万封电子邮件，每个电子邮件的容量也比较大，那么经过一轮邮件炸弹轰炸后电子邮箱的容量可能被占满。
- 另外一方面，这些电子邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞网络；
- 而且邮件服务器需要不停地处理大量的电子邮件，如果承受不了这样的疲劳工作，服务器随时有崩溃的可能。



# DDoS

- ◆ DDoS攻击就是很多DoS攻击源一起攻击某台服务器或网络，迫使服务器停止提供服务或网络阻塞。
- ◆ DDoS攻击需要众多攻击源，而黑客获得攻击源的主要途径就是传播木马，网络计算机一旦中了木马，这台计算机就会被后台操作的人控制，也就成了所谓的“肉鸡”，即黑客的帮凶。
- ◆ 使用“肉鸡”进行DDoS攻击还可以在在一定程度上保护攻击者，使其不易被发现。

## 4 欺骗类攻击

- ◆ 欺骗类攻击是指构造虚假的网络消息，发送给网络主机或网络设备，企图用假消息替代真实信息，实现对网络及主机正常工作的干扰破坏。
- ◆ 常见的假消息攻击有IP欺骗、ARP欺骗、DNS欺骗、伪造电子邮件等



## 5 利用型攻击

- ◆ 利用型攻击是通过非法技术手段，试图获得某网络计算机的控制权或使用权，达到利用该机从事非法行为的一类攻击行为的总称。
- ◆ 利用型攻击常用的技术手段主要包括：
  - 口令猜测、木马病毒、僵尸病毒以及缓冲区溢出等。

# 僵尸病毒

- ◆ 僵尸病毒（Bot）是通过特定协议的信道连接僵尸网络服务器的客户端程序，
  - 被安装了僵尸程序的机器称为僵尸主机，
  - 僵尸网络（BotNet）是由这些受控的僵尸主机依据特定协议所组成的网络。
- ◆ 僵尸病毒的程序结构与木马程序基本一致，
  - 木马程序是被控制端连接的服务器端程序，
  - 僵尸程序是向控制服务器发起连接的客户端程序。
- ◆ 僵尸病毒的传播和木马相似
  - 途径包括电子邮件、含有病毒的WEB网页、捆绑了僵尸程序的应用软件以及利用系统漏洞攻击加载等。
- ◆ 黑客经常利用其发起大规模的网络攻击，
  - 如分布式拒绝服务攻击（DDoS）、海量垃圾邮件等，

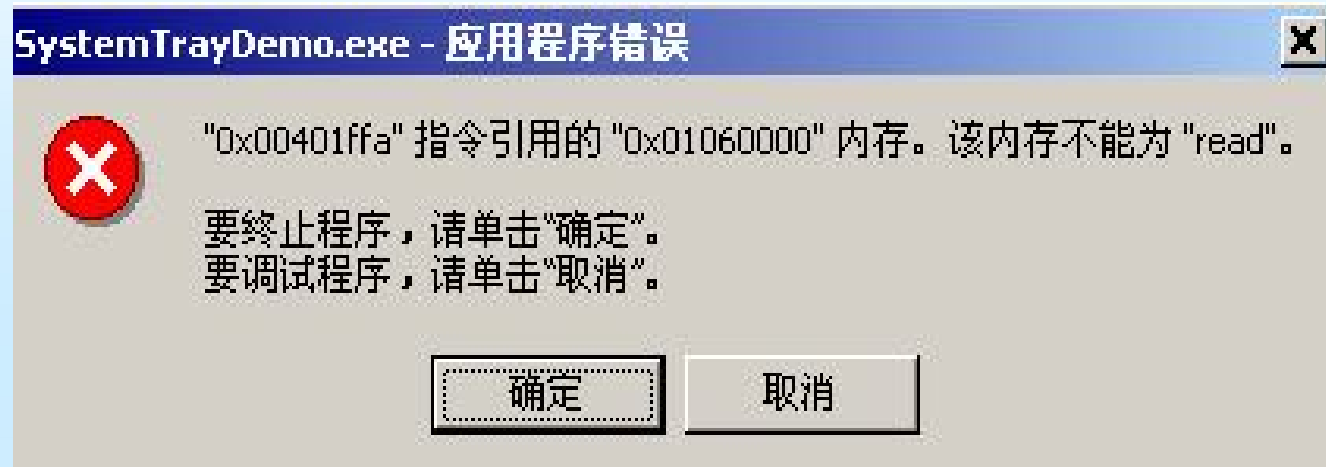


# 缓冲区溢出

- ◆ 缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖了合法数据。
- ◆ 缓冲区溢出是一种非常普遍、非常危险的程序漏洞，在各种操作系统、应用软件中广泛存在。
- ◆ 利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果，更为严重的是可以利用它执行非授权指令，甚至可以取得系统特权并控制主机，进行各种非法操作。



# 程序溢出时的表现



Segmentation Fault (core dumped)



# 缓冲区的理论基础

- ◆ 缓冲区溢出的产生存在着必然性，现代计算机程序的运行机制、C语言的开放性及编译问题是其产生的理论基础。
  - 程序在4GB或更大逻辑地址空间内运行时，一般会被装载到相对固定的地址空间，使得攻击者可以估算用于攻击的代码的逻辑地址；
  - 程序调用时，可执行代码和数据共同存储在一个地址空间（堆栈）内，攻击者可以精心编制输入的数据，通过运行时缓冲区溢出，得到运行权；
  - CPU call调用时的返回地址和C语言函数使用的局部变量均在堆栈中保存，而且C语言不进行数据边界检察，当数据被覆盖时也不能被发现。





# 例子

```
#include <stdio.h>
#include <string.h>
void Sayhello(char* name)
{
    char tmpName [8];
    strcpy(tmpName, name);
    printf("Hello %s\n", tmpName);
}
```

- int main(int argc, char\*\* argv)
- {
- Sayhello(argv[1]);
- return 0;
- }

下面内容是在Linux环境下  
example.c程序的执行情况:

\$ ./ example computer

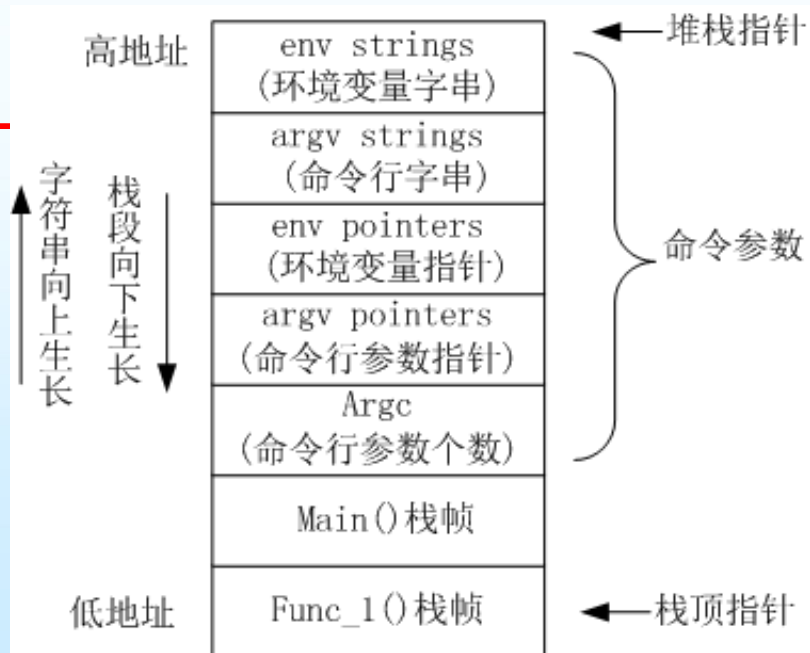
Hello computer

\$ ./ example computersssssssss

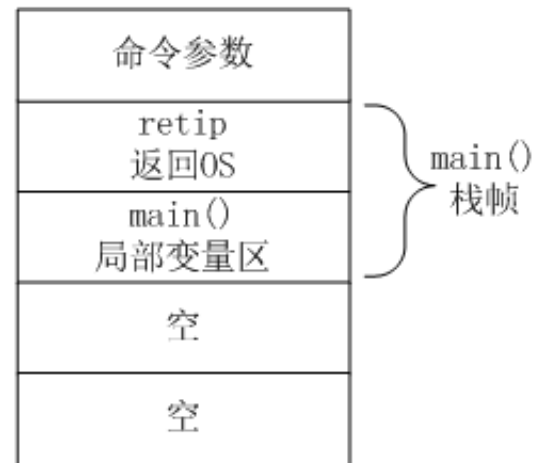
Hello computersssssssss

Segmentation fault (core dumped)

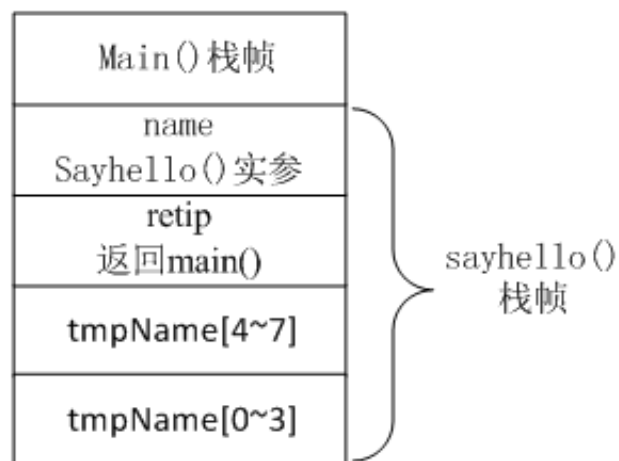
# 分析



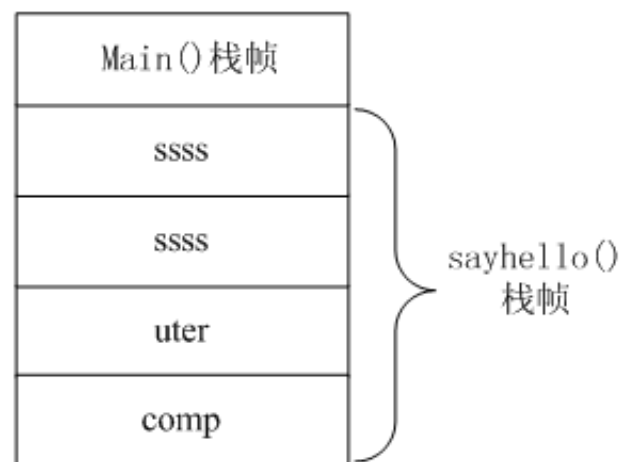
a. 程序执行时栈段分配



b. sayhello() 调用之前



c. sayhello() 正常调用



d. sayhello() 产生溢出



# 主要内容

- ◆ 6.1 概述
- ◆ 6.2 计算机病毒
- ◆ 6.3 网络入侵
- ◆ 6.4 **诱骗类威胁**



## 6.4 诱骗类威胁

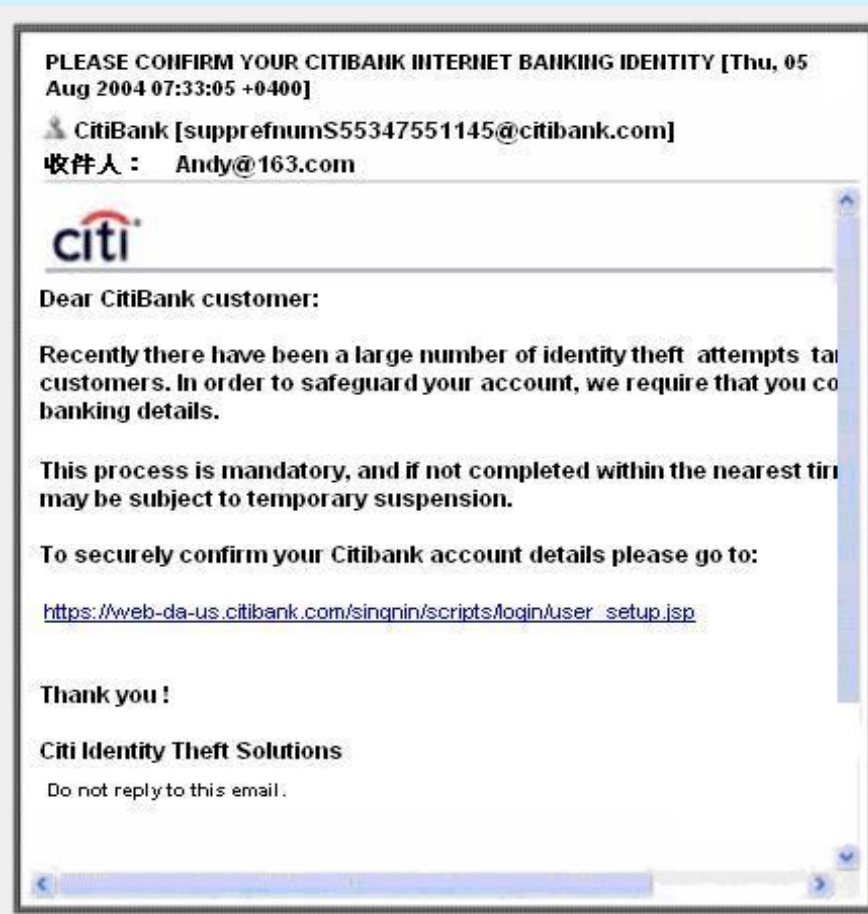
- ◆ 诱骗类威胁是指攻击者利用社会工程学的思想，利用人的弱点（如人的本能反应、好奇心、信任、贪便宜等）通过网络散布虚假信息，诱使受害者上当受骗，而达到攻击者目的的一种网络攻击行为。
- ◆ 准确地说，社会工程学不是一门科学，而是一门艺术和窍门，它利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你受骗上当。

## 6.4.1 网络钓鱼

- ◆ Phishing是英单词Fishing（钓鱼）和Phone（电话，因为黑客起初以电话作案）的综合体，所以被称为网络钓鱼。
- ◆ Phishing是指攻击者通过伪造以假乱真的网站和发送诱惑受害者按攻击者意图执行某些操作的电子邮件等方法，使得受害者“自愿”交出重要信息（例如银行账户和密码）的手段。

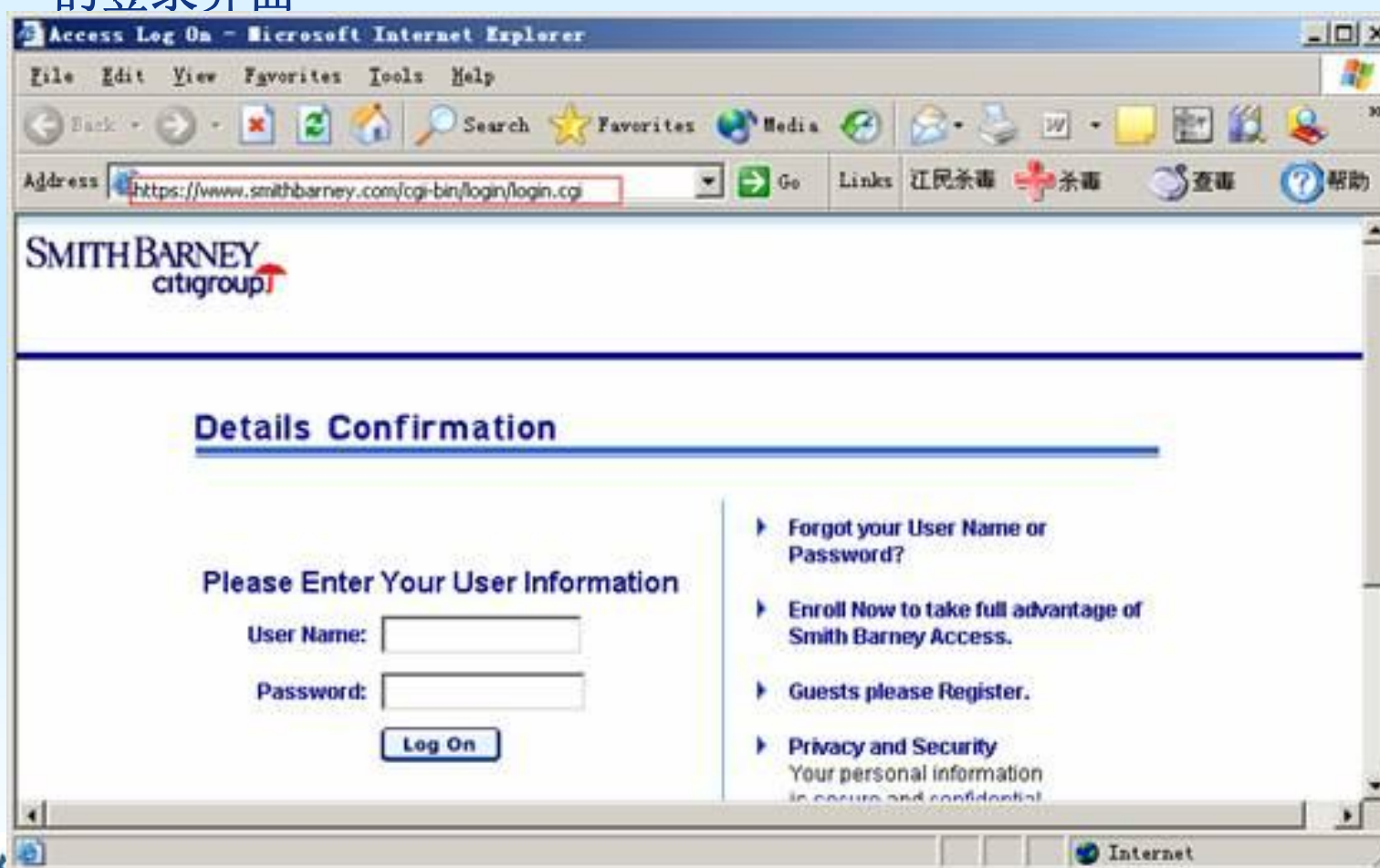
# 社会工程

- ◆ 下面是一个典型的利用社会工程学进行攻击的例子。
- ◆ 某人在某一天收到一封来自花旗银行(CitiBank)的信。上面说，近来在花旗分行的账户不安全，为了保护账户，请到下面的网站上确认一下，并输入信息。



# 社会工程

- ◆ 当用户点击链接时，实际连接的是钓鱼网站  
[http://\\*\\*.41.155.60:87/s](http://**.41.155.60:87/s)。该网站页面酷似Smith Barney银行网站的登录界面



---

*Any question?*

