


第6章 网络威胁

翟健宏

主要内容

6.1 网络威胁概述
6.2 计算机病毒
6.3 网络入侵
6.4 诱骗类威胁
6.5 夺旗赛CTF

6.1 网络威胁概述

6.1.1 什么网络威胁

- **威胁：**用威力逼迫恫吓使人屈服。
- **网络威胁：**是指网络安全受到威胁、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。

6.1.2 网络威胁的四个阶段

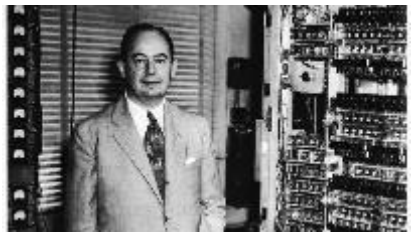
- 第一阶段（1998年以前）网络威胁主要来源于传统的计算机病毒，通过媒介复制进行传染，攻击破坏个人电脑；
- 第二阶段（大致在1998年以后）网络威胁主要以蠕虫病毒和黑客攻击为主，其表现为蠕虫病毒通过网络大面积爆发及黑客攻击一些服务网站；
- 第三阶段（2005年以来）网络威胁多样化，多数以偷窃资料、控制利用主机等手段谋取经济利益为目的。
- 第四阶段（2010年以来）国家级网络战，高级可持续威胁APT，震网stuxnet。

6.1.3 网络威胁分类

网 络 新 战 士

- 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。

6.1.4 计算机病毒



- 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。
- 上世纪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

- 计算机病毒发展趋势

① 无国界
② 多样化
③ 破坏性更强
④ 智能化
⑤ 更加隐蔽化

主要内容

6.1 网络威胁概述

6.2 计算机病毒

6.3 网络入侵

6.4 诱骗类威胁

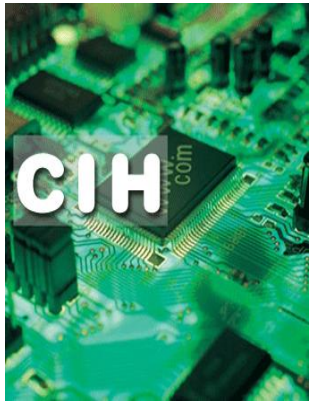
6.5 夺旗赛CTF

6.2 计算机病毒

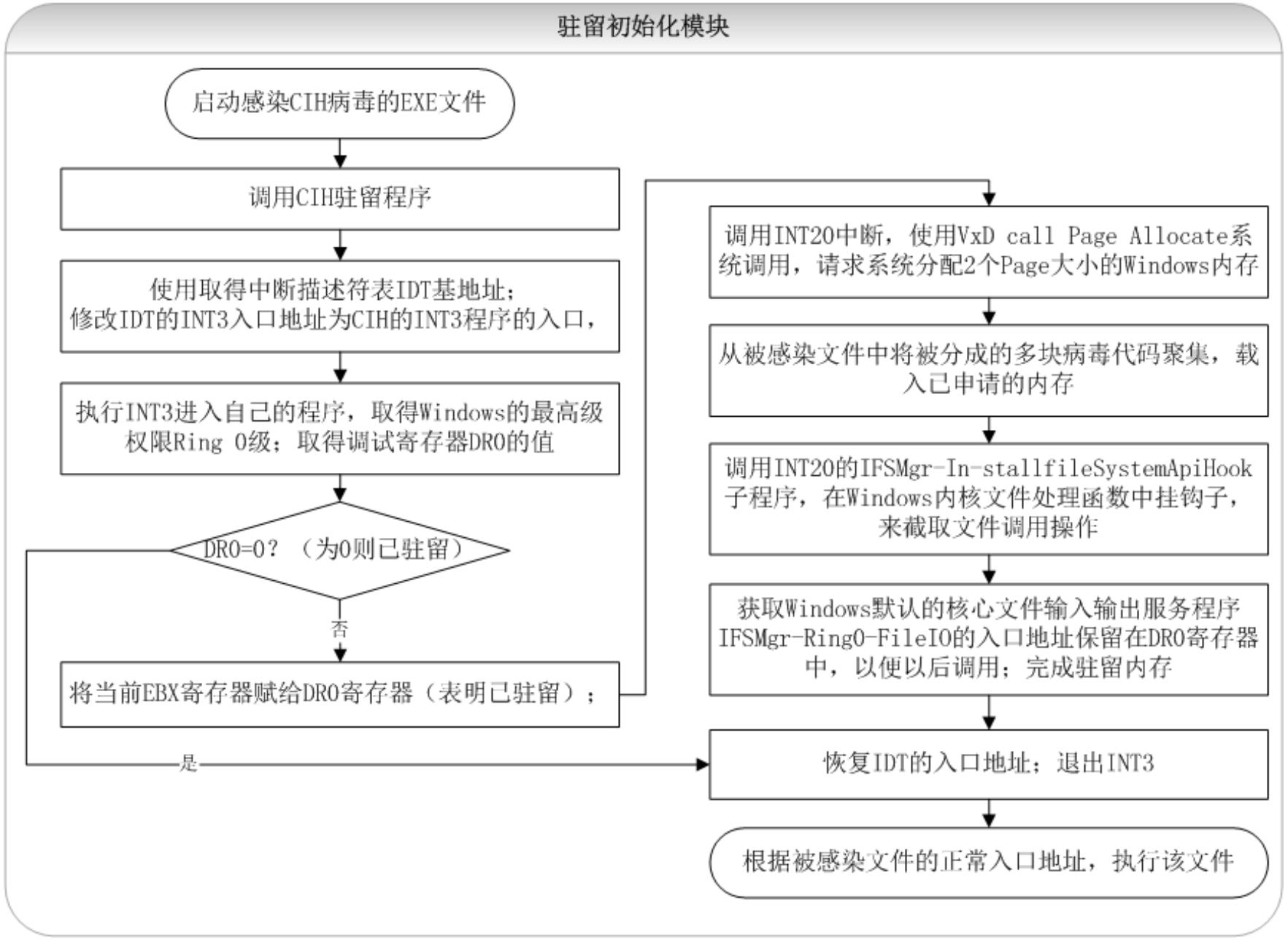
- 计算算机病毒可以根据其工作原理和传播方式划分成三类

6.2.1 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等。
- 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Wnidows核心内存里，
  - 组成：初始化驻留模块、传染模块和破坏模块。

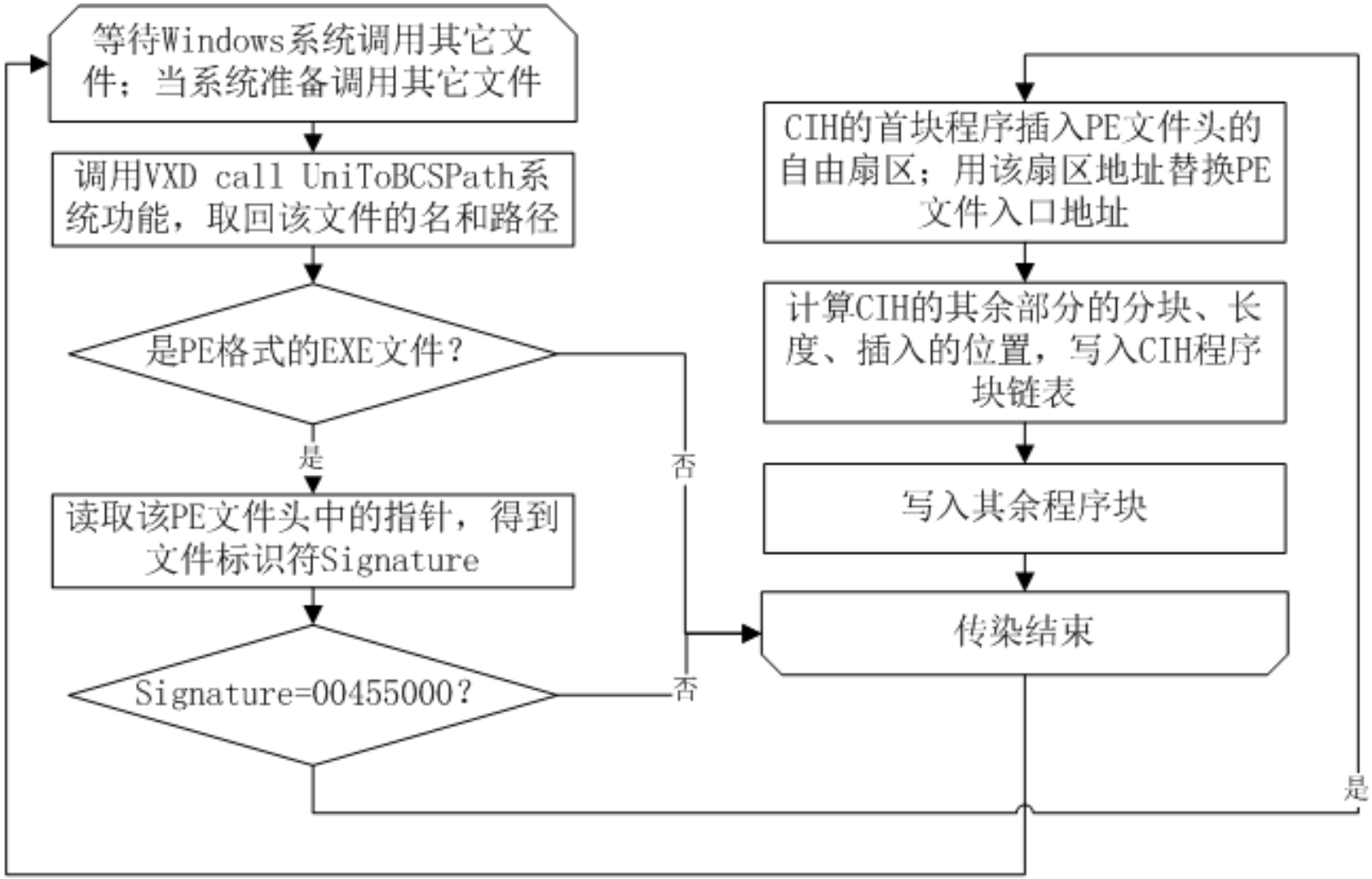


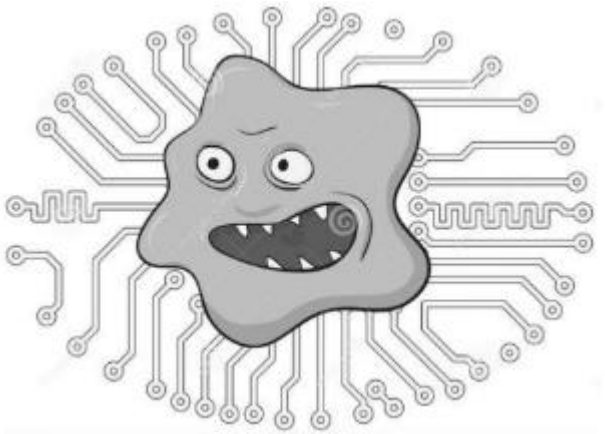
驻留初始化模块

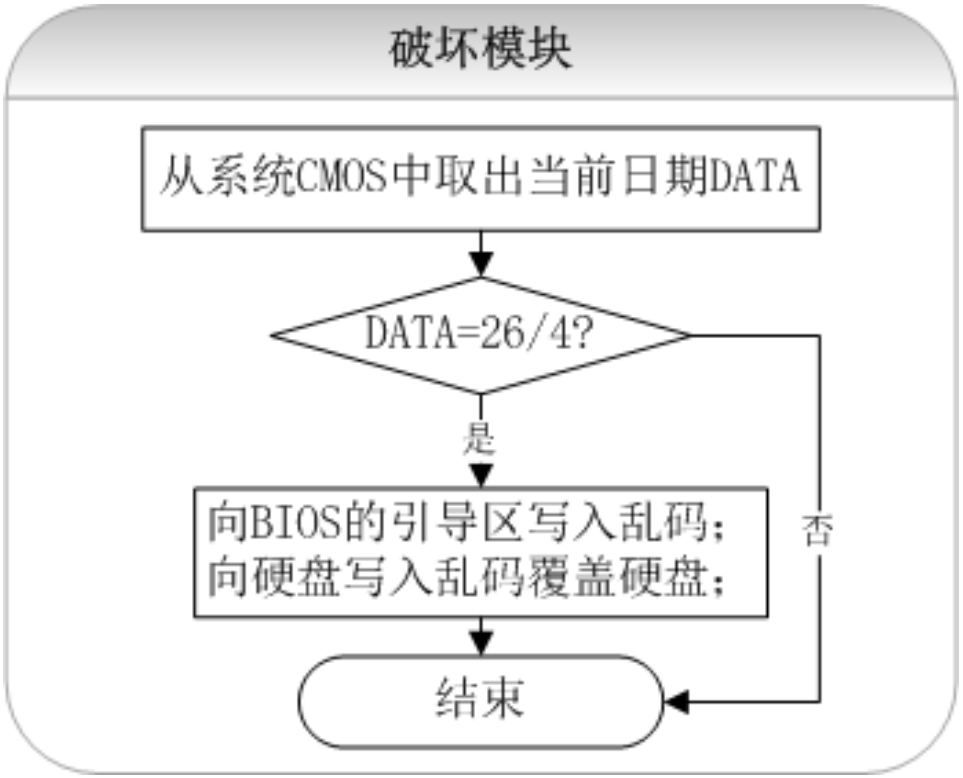

启动感染CIH病毒的EXE文件
调用CIH驻留程序
使用取得中断描述符表IDT基地址；
修改IDT的INT3入口地址为CIH的INT3程序的入口，
执行INT3进入自己的程序，取得Windows的最高级权限Ring 0级；取得调试寄存器DR0的值
DR0=0？（为0则已驻留）
否
将当前EBX寄存器赋给DR0寄存器（表明已驻留）；
是
调用INT20中断，使用VxD call Page Allocate系统调用，请求系统分配2个Page大小的Windows内存
从被感染文件中将被分成的多块病毒代码聚集，载入已申请的内存
调用INT20的IFSMgr-In-stallfileSystemApiHook子程序，在Windows内核文件处理函数中挂钩子，来截取文件调用操作
获取Windows默认的核心文件输入输出服务程序IFSMgr-Ring0-FileIO的入口地址保留在DR0寄存器中，以便以后调用；完成驻留内存
恢复IDT的入口地址；退出INT3
根据被感染文件的正常入口地址，执行该文件


Kingston KVR
GENUINE KINGSTON

传染模块


等待Windows系统调用其它文件；当系统准备调用其它文件
调用VXD call UniToBCSPath系统功能，取回该文件的名和路径
是PE格式的EXE文件？
是
否
读取该PE文件头中的指针，得到文件标识符Signature
Signature=00455000?
否
CIH的首块程序插入PE文件头的自由扇区；用该扇区地址替换PE文件入口地址
计算CIH的其余部分的分块、长度、插入的位置，写入CIH程序块链表
写入其余程序块
传染结束
是




破坏模块
从系统CMOS中取出当前日期DATA
DATA=26/4?
是
否
向BIOS的引导区写入乱码；
向硬盘写入乱码覆盖硬盘；
结束

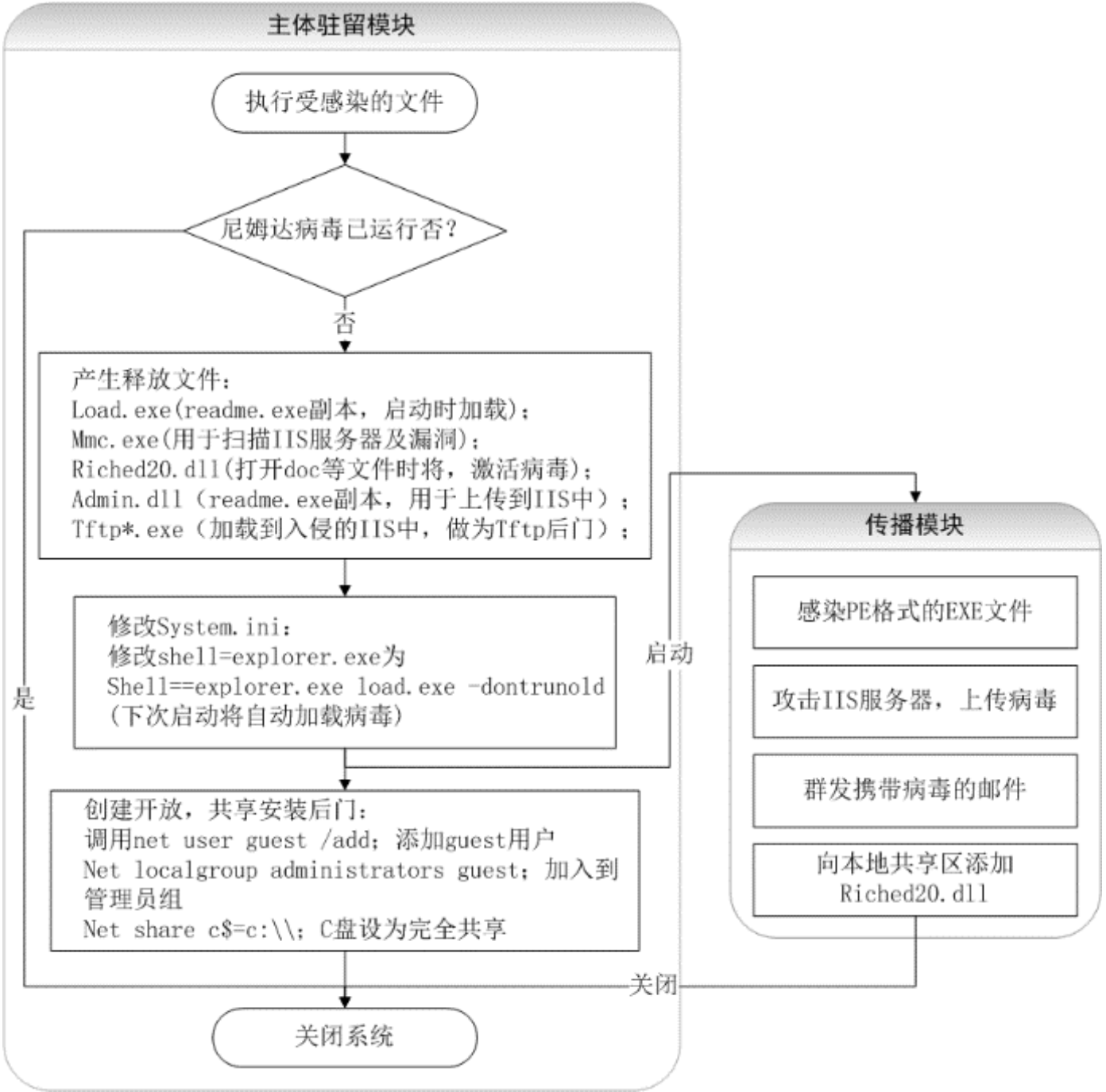
6.2.2 蠕虫病毒

- 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。

尼姆达蠕虫Worms.Nimda

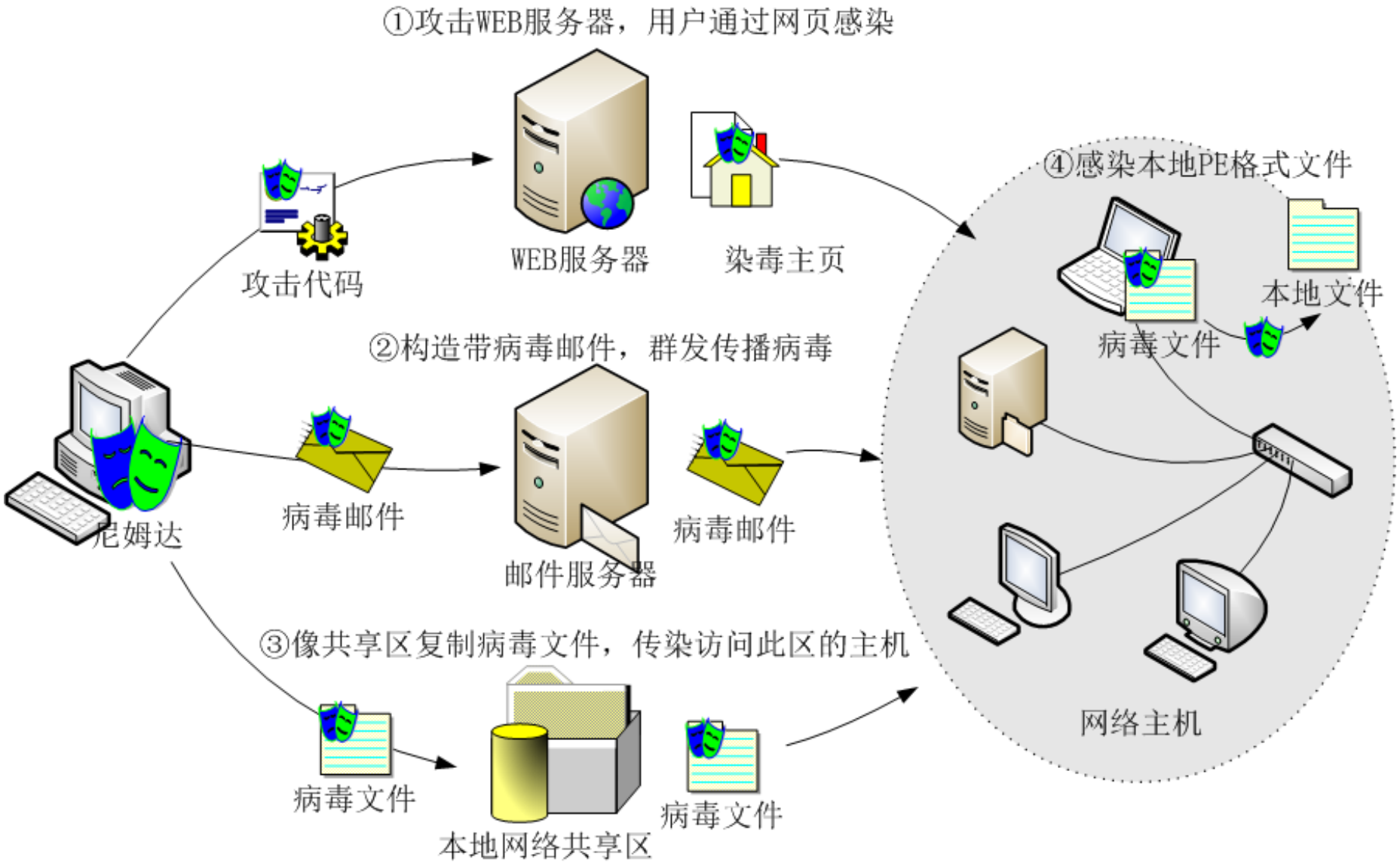
- 2001年9月18日尼姆达病毒在全球蔓延，它能够通过多种传播渠道进行传播，传染性极强，同时破坏力也极大。
  - 尼姆达病毒是一个精心设计的蠕虫病毒，其结构复杂堪称近年来之最。
  - 尼姆达病毒激活后，使用其副本替换系统文件；将系统的各驱动器设为开放共享，降低系统安全性；创建Guest账号并将其加入到管理员组中，安装Guest用户后门。
  - 由于尼姆达病毒通过网络大量传播，产生大量异常的网络流量和大量的垃圾邮件，网络性能势必受到严重影响。

尼姆达病毒程序


主体驻留模块
执行受感染的文件
尼姆达病毒已运行否？
是
否
产生释放文件：
Load.exe(readme.exe副本，启动时加载)；
Mmc.exe(用于扫描IIS服务器及漏洞)；
Riched20.dll(打开doc等文件时将，激活病毒)；
Admin.dll（readme.exe副本，用于上传到IIS中）；
Tftp*.exe（加载到入侵的IIS中，做为Tftp后门）；
修改System.ini：
修改shell=explorer.exe为
Shell==explorer.exe load.exe -dontrunold
（下次启动将自动加载病毒）
创建开放，共享安装后门：
调用net user guest /add；添加guest用户
Net localgroup administrators guest；加入到管理员组
Net share c$=c:\\；C盘设为完全共享
关闭
关闭系统
启动
传播模块
感染PE格式的EXE文件
攻击IIS服务器，上传病毒
群发携带病毒的邮件
向本地共享区添加Riched20.dll

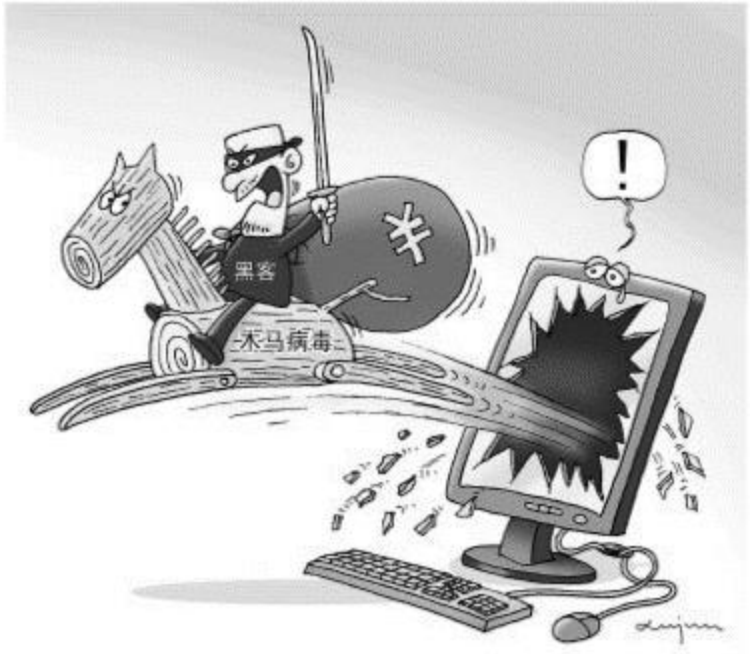

NIMDA
1
2
3
4
.exe
E-mail
www
Lan

Nimda 传播途径


①攻击WEB服务器，用户通过网页感染
攻击代码
WEB服务器
染毒主页
④感染本地PE格式文件
本地文件
病毒文件
②构造带病毒邮件，群发传播病毒
尼姆达
病毒邮件
邮件服务器
病毒邮件
③像共享区复制病毒文件，传染访问此区的主机
病毒文件
本地网络共享区
病毒文件
网络主机

6.2.3 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

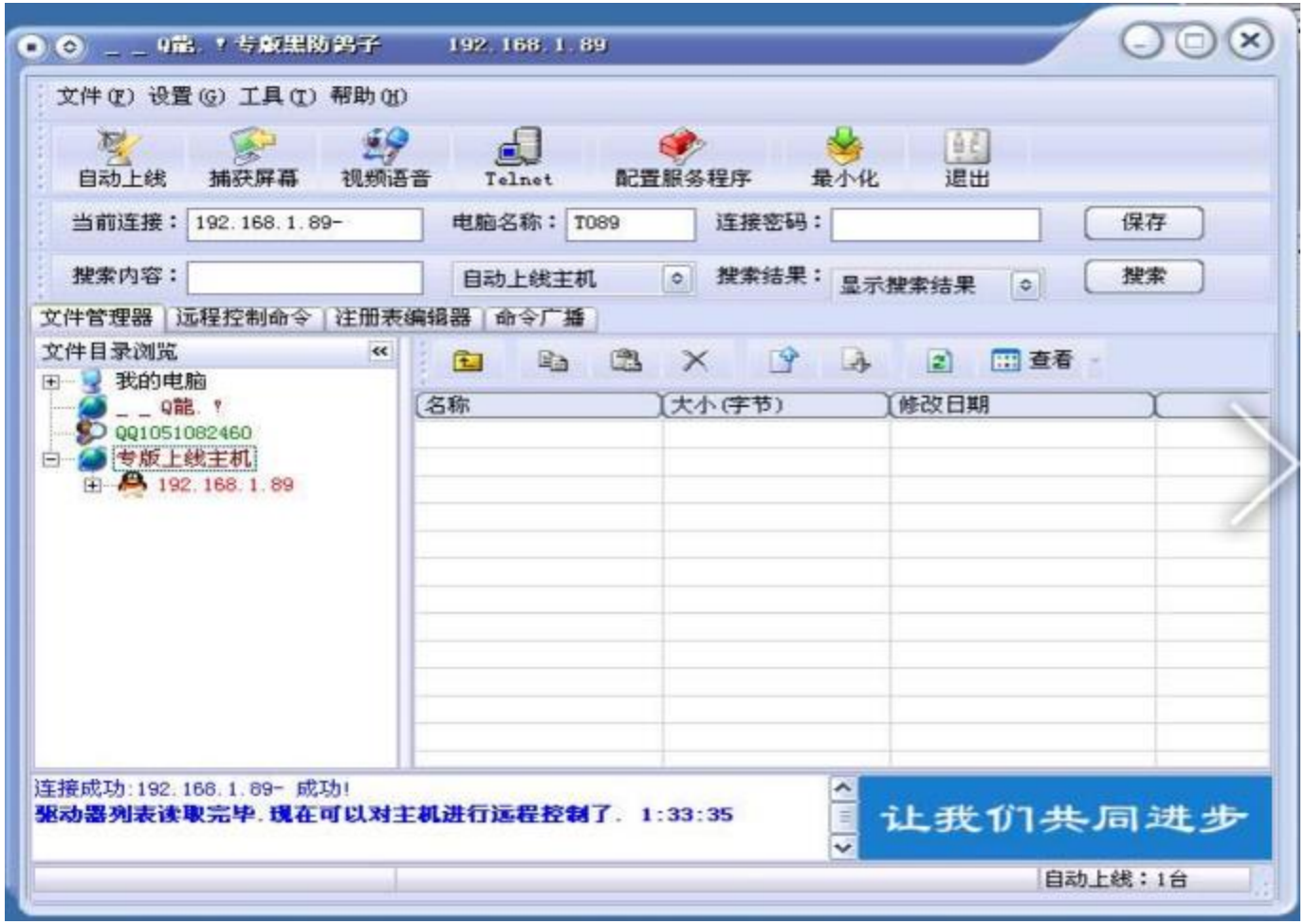
(1) 盗号类木马
(2) 网页点击类木马
(3) 下载类木马
(4) 代理类木马

木马病毒程序组成

- 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。

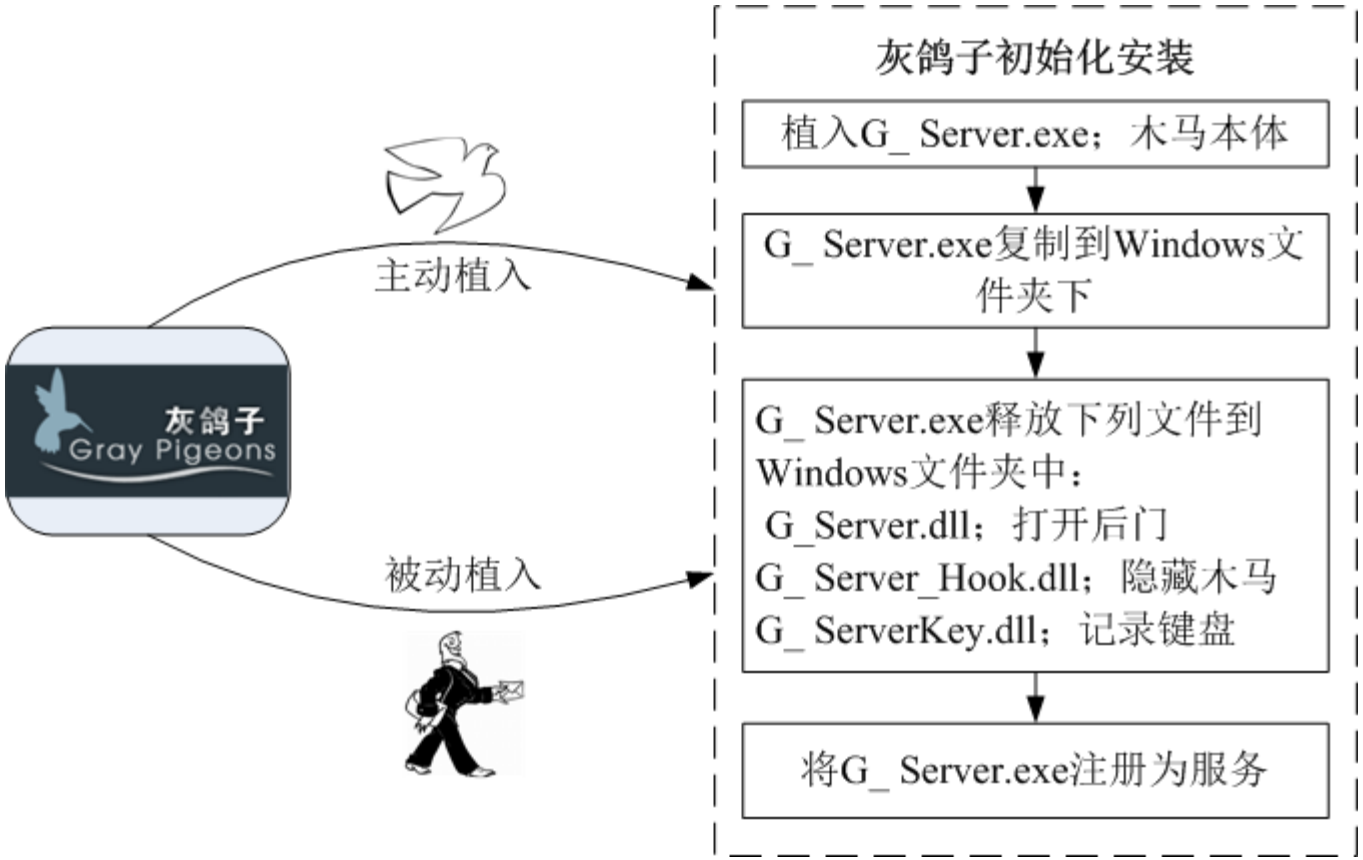
灰鸽子木马

灰鸽子木马，2001，灰鸽子实验室



灰鸽子木马的传播方法

- 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。



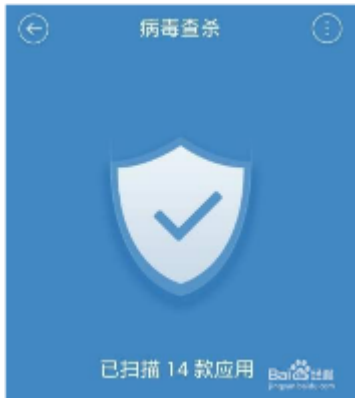
客户端程序

- 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，服务器端文件的名字默认为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

灰鸽子的隐藏技术

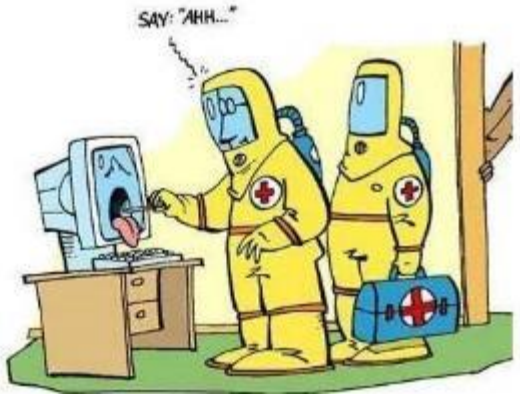
- 隐藏文件
- 隐藏进程
- 隐藏通讯
  - 通讯端口复用技术是指将自己的通讯直接绑定到正常用户进程的端口，接收数据后，根据包格式判断是不是自己的，如果是它的，自己处理，否则通过127.0.0.1的地址交给真正的服务器应用进行处理。
  - 反弹端口技术是指木马程序启动后主动连接客户，为了隐蔽起见，控制端的被动端口一般设置为80端口。对内部网络到外部网络的访问请求，防火墙一般不进行过于严格的检查，加之其连接请求有可能伪造成对外部资源的正常访问，因此可以通过防火墙。

6.2.4 计算机病毒防治

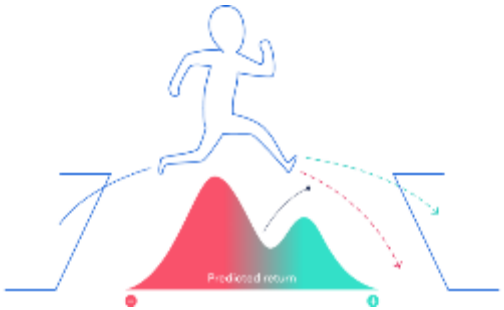


- 病毒防治技术略滞后于病毒技术
- 对于大多数计算机用户来说，防治病毒首先需要选择一个有效的防病毒产品，并及时进行产品升级。
- 计算机病毒防治技术主要包括:
  - 检测、清除、预防和免疫。
  - 检测和清除是根治病毒的有力手段，
  - 预防和免疫也是保证计算机系统安全的重要措施

检测



- 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。
- 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。
- 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。



- **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。
- **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。

计算机中毒的常见症状

- 系统运行速度减慢;
- 系统经常无故发生死机
- 文件长度发生变化;
- 存储的容量异常减少;
- 丢失文件或文件损坏;
- 屏幕上出现异常显示;
- 系统的蜂鸣器出现异常声响;
- 磁盘卷标发变化;
- 系统不识别硬盘;
- 对存储系统异常访问;
- 键盘输入异常;
- 文件的日期、时间、属性等发生变化;
- 文件无法正确读取、复制或打开;
- 命令执行出现错误;
- WINDOWS操作系统无故频繁出现错误;
- 系统异常重新启动;
- 一些外部设备工作异常;
- 出现异常的程序驻留内存

清除

- **清除病毒主要分为**
  - 使用防病毒软件和手工清除病毒两种方法。
  - 防病毒软件由安全厂商精心研制，可以有效查杀绝大多数计算机病毒，多数用户应采用防病毒软件来清除病毒。
    - 防病毒软件对检测到的病毒一般采取三种处理方案，分别是清除、隔离和删除。
    - 清除是指在发现文件被感染病毒时，采取的清除病毒并保留文件的动作。
    - 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。

蠕虫、木马等病毒的清除

- **结束所有可疑进程**
- **删除病毒文件并恢复注册表**
- **内核级后门的清除**
- **重启后扫描**
  - 完成了上述三步，随后需要重新启动系统，并使用带有最新病毒库的防病毒软件对全盘进行扫描（这一步非常重要，做不好的话前功尽弃）

预防

- 安装防毒软件
  - 打开你的防毒软件的自动升级服务，定期扫描计算机
- 注意软盘、光盘以及U盘等存储媒介
  - 在使用软盘、光盘、U盘或活动硬盘前，病毒扫描
- 关注下载安全
  - 下载要从比较可靠的站点进行，下载后做病毒扫描。
- 关注电子邮件安全
  - 来历不明的邮件决不要打开，决不要轻易运行附件
- 使用基于客户端的防火墙
- 警惕欺骗性的病毒
- 备份

免疫

- 计算机病毒免疫
  - 提高计算机系统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；

注射“病毒疫苗”

- 实施免疫的主要方法包括以下几个方面：
  - 感染标识免疫
    - 人为地为正常对象中加上病毒感染标识，使计算机病毒误以为已经感染从而达到免疫的目的。
  - 文件扩展名免疫
    - 将扩展名改为非COM、EXE、SYS、BAT等形式，
    - 将系统默认的可执行文件的后缀名改为非COM、EXE、SYS、BAT等形式。
  - 外部加密免疫
    - 外部加密免疫是指在文件的存取权限和存取路径上进行加密保护，以防止文件被非法阅读和修改。
  - 内部加密免疫
    - 对文件内容加密变换后进行存储，在使用时再进行解密。

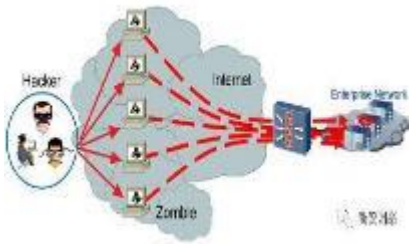
主要内容

6.1 网络威胁概述
6.2 计算机病毒
6.3 网络入侵
6.4 诱骗类威胁
6.5 夺旗赛CTF

6.3 网络入侵

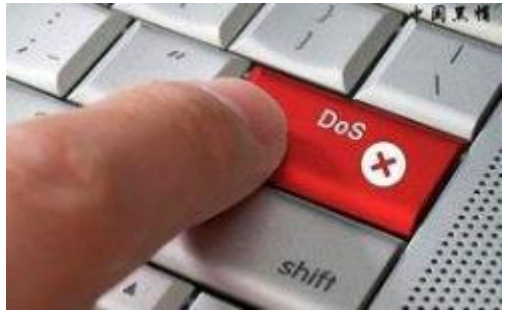
- 1980年，James P Anderson首次提出了“入侵”的概念。
  - “入侵”是指在非授权的情况下，试图存取信息、处理信息或破坏系统，以使系统不可靠或不可用的故意行为。
  - 网络入侵一般是指具有熟练编写、调试和使用计算机程序的技巧的人，利用这些技巧来获得非法或未授权的网络或文件的访问，进入内部网的行为。
  - 对信息的非授权访问一般被称为破解cracking。

网络入侵



- 入侵过程：前期准备、实施入侵和后期处理。
  - **准备阶段**需要完成的工作主要包括明确入侵目的、确定入侵对象以及选择入侵手段，
    - 入侵目的一般可分为控制主机、瘫痪主机和瘫痪网络；
    - 入侵对象一般分为主机和网络两类；
    - 根据目的和后果分为：拒绝服务攻击、口令攻击、嗅探攻击、欺骗攻击和利用型攻击。
  - **实施入侵**阶段是真正的攻击阶段，主要包括扫描探测和攻击。
    - 扫描探测主要用来收集信息，为下一步攻击奠定基础；
    - 攻击：根据入侵目的、采用相应的入侵手段向入侵对象实施入侵。
  - **后期处理**主要是指由于大多数入侵攻击行为都会留下痕迹，攻击者为了清除入侵痕迹而进行现场清理。

6.3.1 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

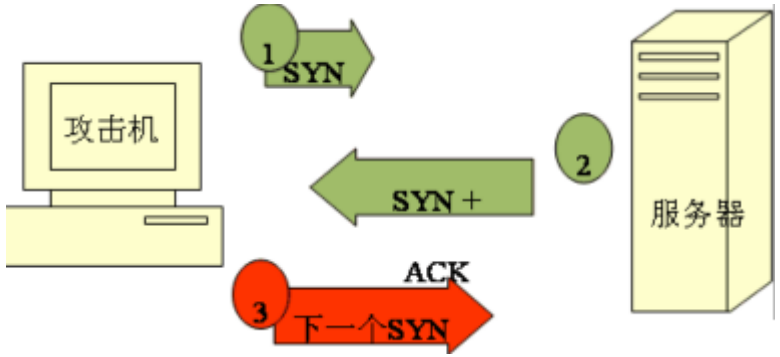
- TCP/IP的规范，一个包的长度最大为65536字节。
- 利用多个IP包分片的叠加能做到构造长度大于65536的IP数据包。
- 攻击者通过修改IP分片中的偏移量和段长度，使系统在接收到全部分段后重组报文时总的长度超过了65535字节。

- 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



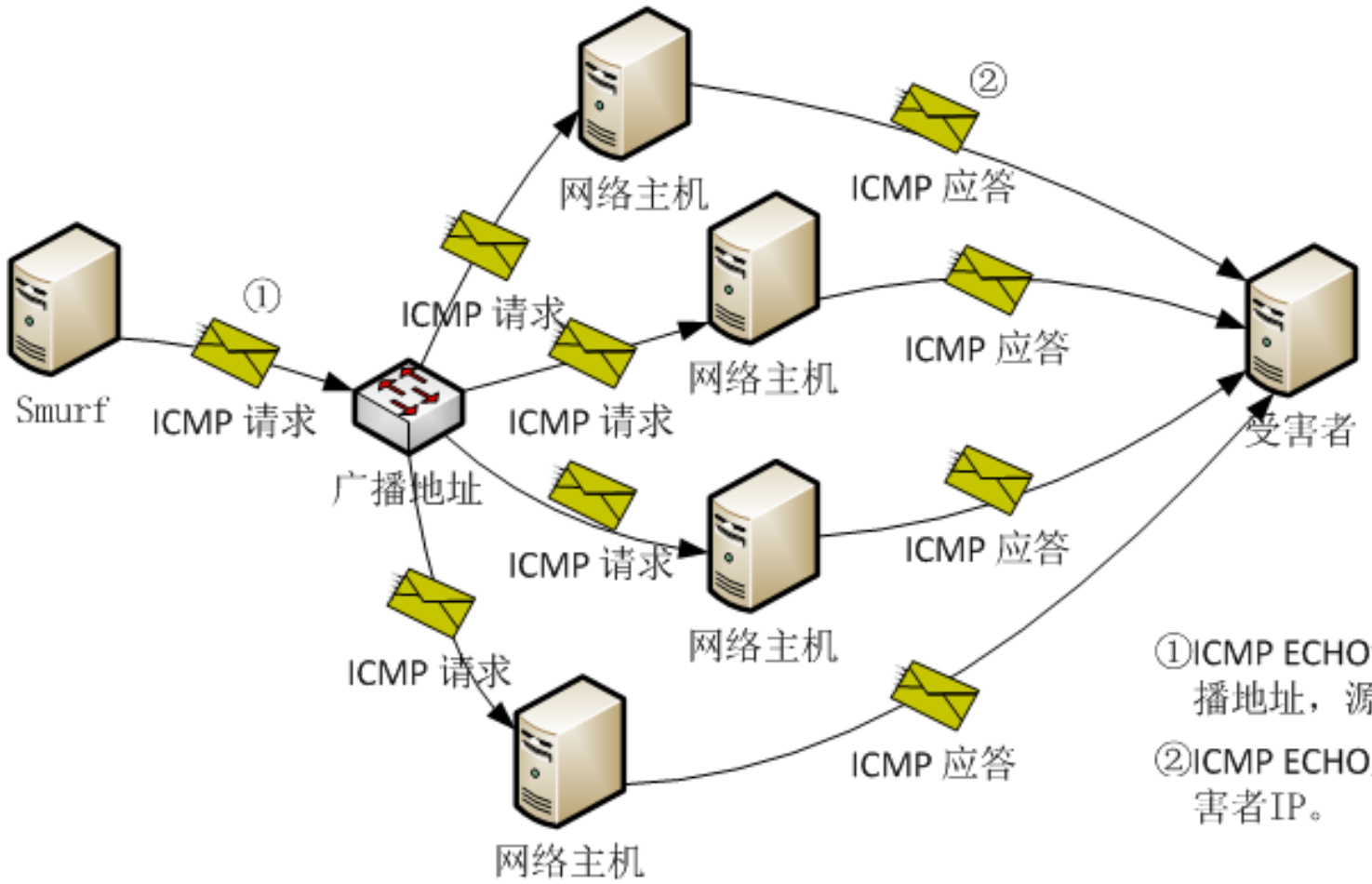
- 攻击者伪造TCP的连接请求，向被攻击的设备正在监听的端口发送大量的SYN连接请求报文；
- 被攻击的设备按照正常的处理过程，回应这个请求报文，同时为它分配了相应的资源。
- 攻击者不需要建立TCP连接，因此服务器根本不会接收到第三个ACK报文，现有分配的资源只能等待超时释放。

- 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会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。

Smurf攻击过程示意图



①ICMP ECHO请求包：目的地址为广播地址，源地址为受害者IP；

②ICMP ECHO应答包：目的地址为受害者IP。

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；
  - 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攻击还可以在一定程度上保护攻击者，使其不易被发现。

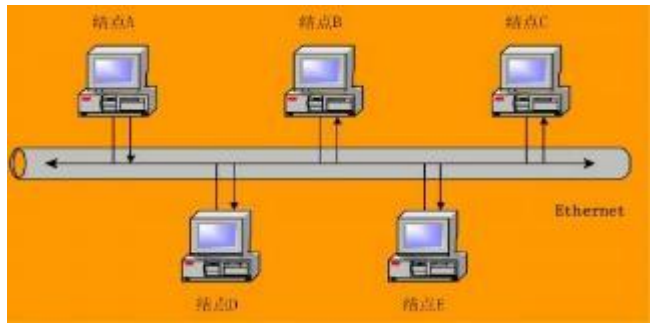
DoS攻击的主要防御方法

- 及时为系统升级，减少系统漏洞，很多DoS攻击对于新的操作系统已经失效，如Ping of Death攻击；
- 关掉主机或网络中的不必要的服务和端口，如对于非WEB主机关掉80端口；
- 局域网应该加强防火墙和入侵检测系统的应用和管理，过滤掉非法的网络数据包。

6.3.2 嗅探攻击

- 嗅探攻击也称为网络嗅探，是指利用计算机的网络接口截获目的地为其它计算机的数据包的一种手段。
- 网络嗅探的工具被称为嗅探器（sniffer），是一种常用的收集网络上传输的有用数据的方法。
- 嗅探攻击一般是指黑客利用嗅探器获取网络传输中的重要数据。网络嗅探也被形象地称为网络窃听。

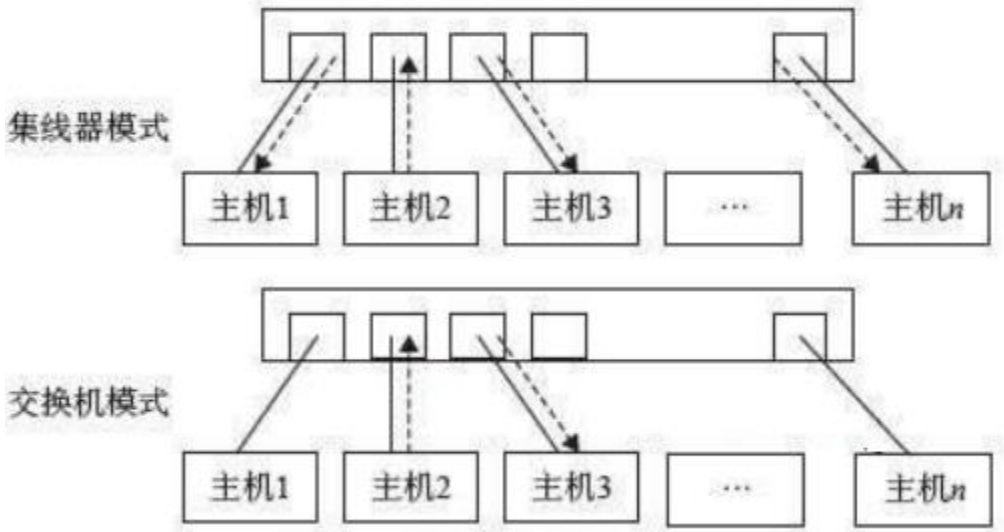
共享网络环境



- 以太网卡共有四种工作方式：
  - 广播方式： 网卡能够接收网络中的广播数据；
  - 组播方式： 网卡能够接收组播数据；
  - 直接方式： 只有目的网卡才能接收该数据；
  - 混杂模式： 网卡能够接收一切通过它的数据。

- 如果攻击者获得其中一台主机的root权限，并将其网卡置于混杂模式，这就意味着不必打开配线盒来安装偷听设备，就可以在对共享环境下的其它计算机的通信进行窃听，
- 在共享网络中网络通信没有任何安全性可言。

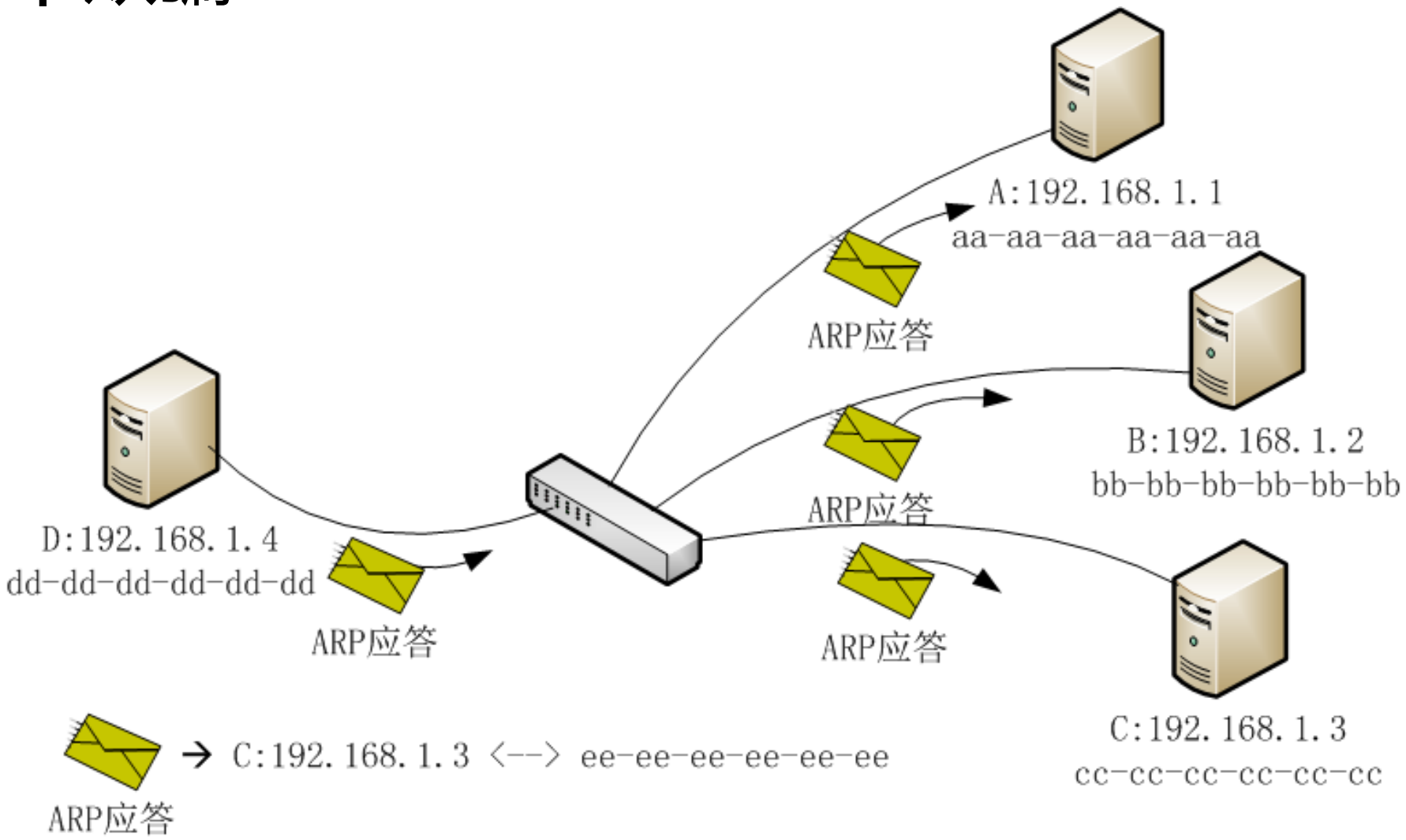
交换网络环境



Internet	地址	物理地址
192.168.1.100	00-30-48-31-26-98	动态
192.168.1.101	00-00-00-00-01-89	动态
192.168.1.102	00-24-dc-b8-47-f0	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态

- Arp协议
  - 当主机接收到ARP应答数据包的时候，就使用应答数据包内的数据对本地的ARP缓存进行更新或添加。

Arp欺骗


A:192.168.1.1
aa-aa-aa-aa-aa-aa
ARP应答
B:192.168.1.2
bb-bb-bb-bb-bb-bb
ARP应答
D:192.168.1.4
dd-dd-dd-dd-dd-dd
ARP应答
ARP应答
C:192.168.1.3
cc-cc-cc-cc-cc-cc
ARP应答
C:192.168.1.3 <--> ee-ee-ee-ee-ee-ee

防范嗅探攻击

- 检测嗅探器
  - 检测混杂模式网卡来检查嗅探器的存在，AntiSniff。
- 安全的拓扑结构
  - 嗅探器只能在当前网络段上进行数据捕获。将网络分段工作进行得越细，嗅探器能够收集的信息就越少。
- 会话加密
  - 即使嗅探器嗅探到数据报文，也不能识别其内容。
- 地址绑定
  - 在客户端使用arp命令绑定网关的真实MAC地址;
  - 在交换机上做端口与MAC地址的静态绑定;
  - 在路由器上做IP地址与MAC地址的静态绑定;
  - 用静态的ARP信息代替动态的ARP信息。

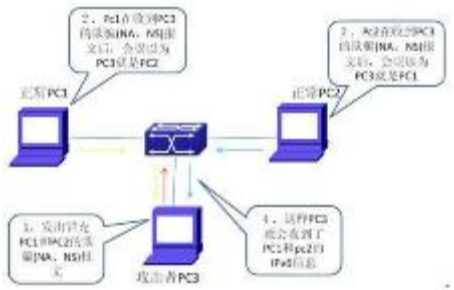
6.3.4 欺骗类攻击

- 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

IP欺骗

- IP欺骗简单地说就是一台主机设备冒充另外一台主机的IP地址，与其它设备通信。
- IP欺骗主要是基于远程过程调用RPC的命令，比如rlogin、rcp、rsh等，
- 这些命令仅仅根据信源IP地址进行用户身份确认，以便允许或拒绝用户RPC。
- IP欺骗的目的主要是获取远程主机的信任及访问特权。

IP欺骗攻击主要步骤



第一步 选定目标主机并发现被该主机信任的其它主机;

第二步 使得被信任的主机丧失工作能力;

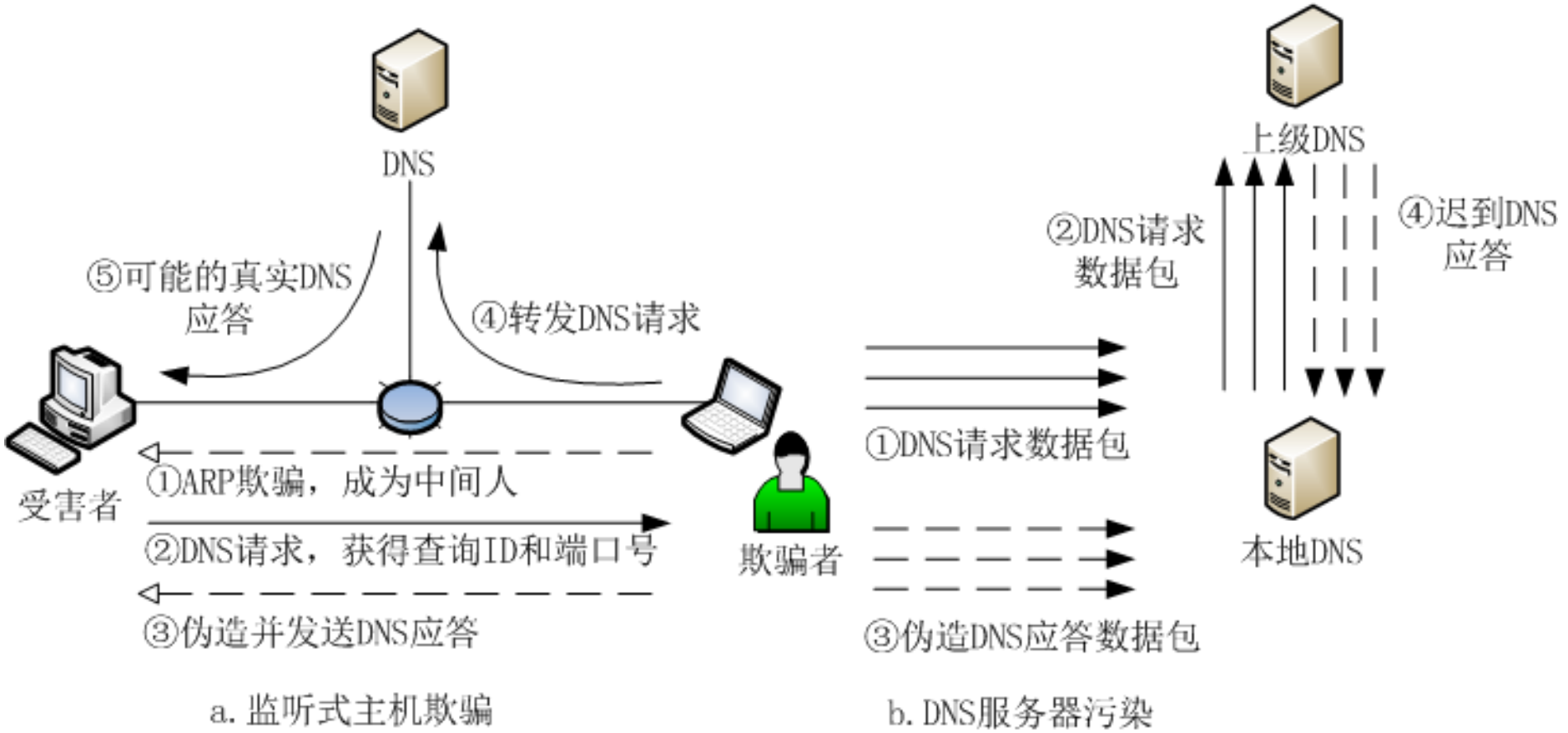
第三步 使用被目标主机信任的主机的IP地址，伪造建立TCP连接的SYN请求报文，试图以此数据报文建立与目标主机的TCP连接;

第四步 序列号取样和猜测。

第五步 使用被目标主机信任的主机的IP地址和计算出的TCP 序列号，构造TCP连接的ACK报文，发送给目标主机，建立起与目标主机基于地址验证的应用连接。

- 如果成功，攻击者可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

DNS欺骗


DNS
⑤可能的真实DNS
应答
④转发DNS请求
受害者
①ARP欺骗，成为中间人
②DNS请求，获得查询ID和端口号
③伪造并发送DNS应答
欺骗者
a. 监听式主机欺骗
上级DNS
②DNS请求
数据包
④迟到DNS
应答
①DNS请求数据包
本地DNS
③伪造DNS应答数据包
b. DNS服务器污染

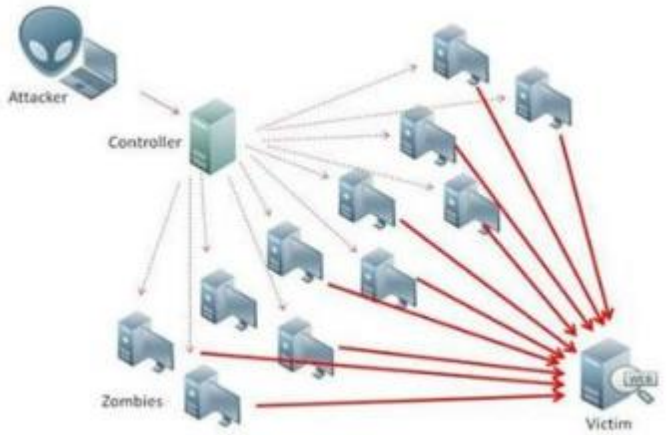
伪造电子邮件

- 由于SMTP并不对邮件的发送者的身份进行鉴定，攻击者可以冒充别的邮件地址伪造电子邮件。
- 攻击者伪造电子邮件的目的主要包括：
  - 攻击者想隐藏自己的身份，匿名传播虚假信息，如造谣中伤某人；
  - 攻击者想假冒别人的身份，提升可信度，如冒充领导发布通知；
  - 伪造用户可能关注的发件人的邮件，引诱收件人接收并阅读，如传播病毒、木马等。

对于欺骗类攻击的防范方法

- 抛弃基于地址的信任策略，不允许使用r类远程调用命令。
- 配置防火墙，拒绝网络外部与本网内具有相同IP地址的连接请求；过滤掉入站的DNS更新。
- 地址绑定，在网关上绑定IP地址和MAC地址；在客户端使用arp命令绑定网关的真实MAC地址命令。
- 使用PGP等安全工具并安装电子邮件证书。

6.3.5 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。

口令攻击

- 口令攻击过程一般包括以下几个步骤。
  - 步骤一、获取目标系统的用户帐号及其它有关信息；
    - 获取目标系统的用户帐号及其它有关信息一般可以利用一些网络服务来实现，如Finger、Whois、LDAP等信息服务。
  - 步骤二、根据用户信息猜测用户口令；
  - 步骤三、采用字典攻击方式探测口令；
    - 使用一些程序，自动地从电脑字典中取出一个单词，作为用户的口令输入给远端的主机，进入系统。
    - 如果口令错误，就按序取出下一个单词，进行下一个尝试。并一直循环下去，直到找到正确的口令或字典的单词试完为止。
    - 由于这个破译过程由计算机程序来自动完成，几个小时就可以把字典的所有单词都试一遍。
  - 步骤四、探测目标系统的漏洞，伺机取得口令文件，破解取得用户口令。

- **暴力攻击口令**

- 系统中可以用作口令的字符有95个，
  - 10个数字、33个标点符号、52个大小写字母。
  - 采用任意5个字母加上一个数字或符号则可能的排列数约为163亿，即$52^5 \times 43 = 16,348,773,000$。
- 这个数字对于每秒可以进行上百万次浮点运算的计算机并不是什么困难问题，也就是说一个6位的口令将不是安全的
- 一般建议使用10位以上并且是字母、数字加上标点符号的混合体。

防范口令攻击的方法

- 口令的长度不少于10个字符;
- 口令中要有一些非字母;
- 口令不在英语字典中;
- 不要将口令写下来;
- 不要将口令存于电脑文件中;
- 不要选择易猜测的信息做口令;
- 不要在不同系统上使用同一口令;
- 不要让其他人得到口令;
- 经常改变口令;
- 永远不要对自己的口令过于自信。

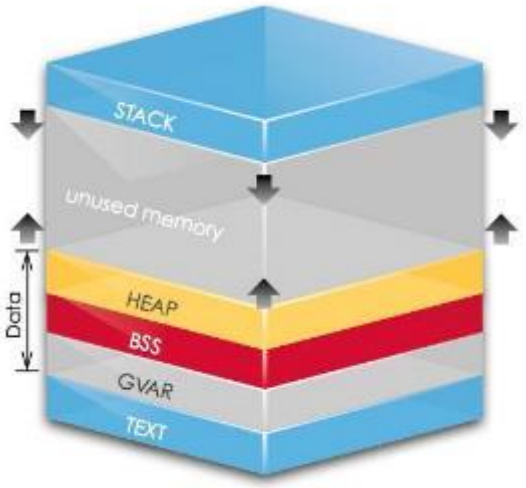
僵尸病毒

- 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。
- 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。

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

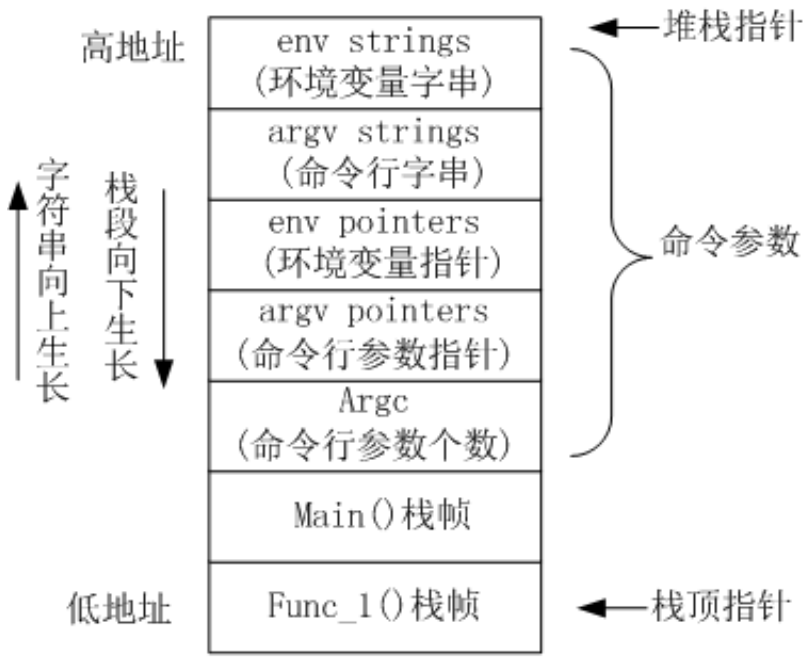
- int main(int argc, char** argv)
- {
- Sayhello(argv[1]);
- return 0;
- }

下面内容是在Linux环境下example.c程序的执行情况：

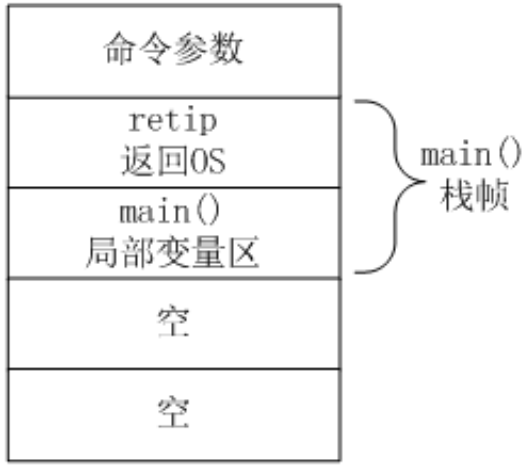
```
$ ./ example computer
Hello computer
$ ./ example computersssssssss
Hello computersssssssss
Segmentation fault (core dumped)
```

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

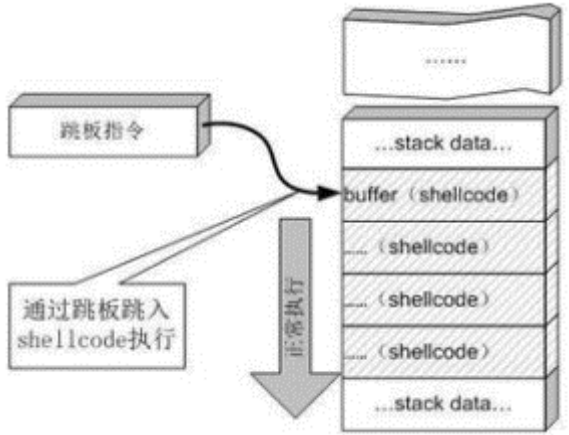
分析

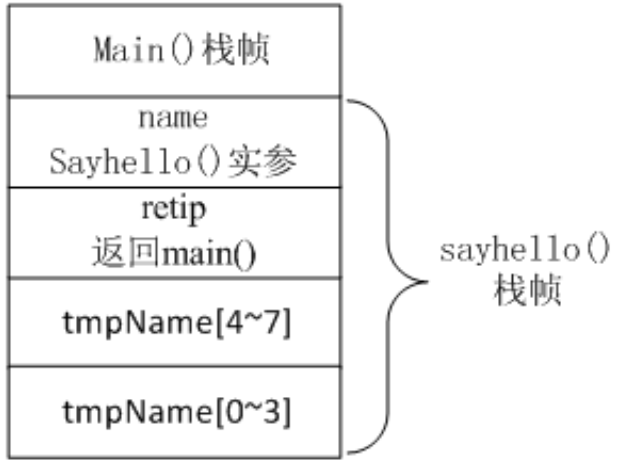


a. 程序执行时栈段分配

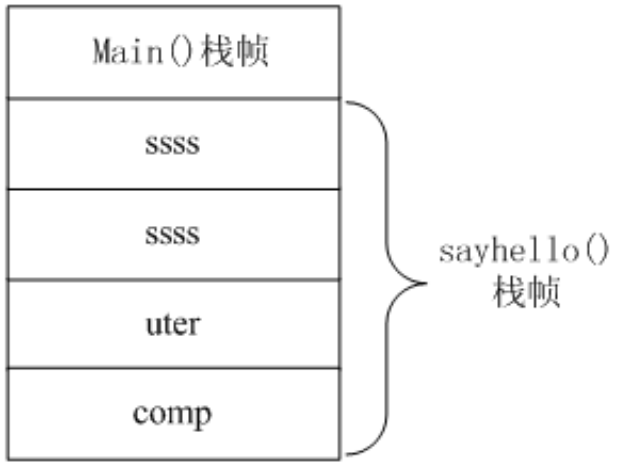


b. sayhello()调用之前





c. sayhello()正常调用



d. sayhello()产生溢出

主要内容

6.1 网络威胁概述
6.2 计算机病毒
6.3 网络入侵
6.4 诱骗类威胁
6.5 夺旗赛CTF

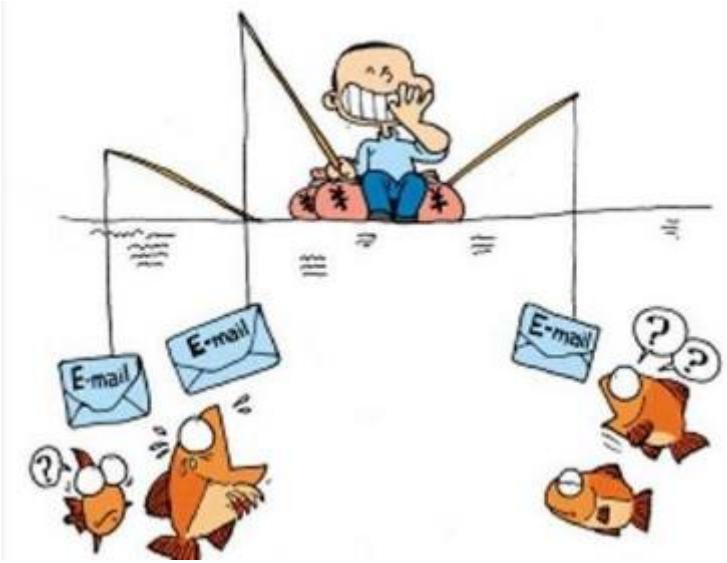
6.4 诱骗类威胁

- 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、恐惧、贪婪等）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。

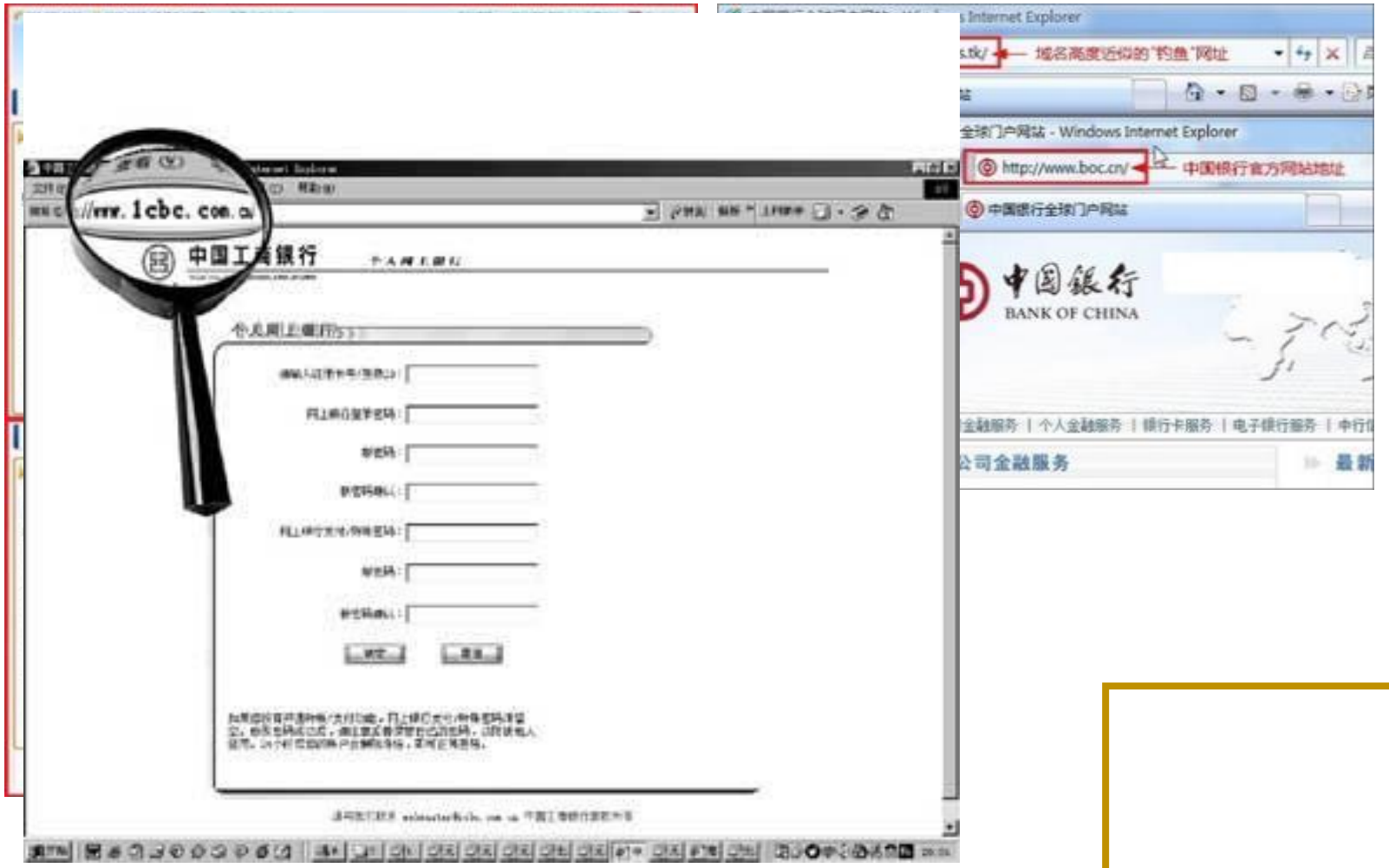
6.4.1 网络钓鱼



- 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。

假冒网站

- 假冒网站，骗取用户帐号、密码实施盗窃，对用户造成经济损失最大的恶劣手段。
- 为了迷惑用户，攻击者有意把网站域名注册成与真实机构的域名很相似：
  - 网址为“http: //www. 1cbc. com. cn”，而真正银行网站是“http: //www. icbc. com. cn”，



虚假的电子商务

- 攻击者建立电子商务网站，或是在比较知名、大型电子商务网站上发布虚假的商品销售信息。

- 网上交易多是异地交易，通常需要汇款。
  - 不法分子一般要求消费者先付部分款，再以各种理由诱骗消费者付余款或者其他各种名目的款项，得到钱款或被识破时，犯罪分子就销声匿迹。

电子邮件诱骗

- 电子邮件服务是合法的Internet经典服务，攻击者进行电子邮件诱骗，一般需要经过以下四个步骤。

  第一步 选定目标用户群。

  第二步 构造欺骗性电子邮件。

  第三步 搭建欺骗性网站。

  第四步 群发邮件，等待上当的受害者。

6.4.2 钓鱼、渔叉与水坑

水坑攻击water hole attack：

指黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待被攻击者来访时实施攻击。

6.4.3 对于诱骗类威胁的防范

- 诱骗类威胁不属于传统信息安全的范畴，传统信息安全办法解决不了非传统信息安全的威胁。
  - 一般认为，解决非传统信息安全威胁需要运用社会工程学来反制。
  - 防范诱骗类威胁的首要方法是加强安全防范意识，多问“为什么”，减少“天上掉馅饼”的心理，那么绝大多数此类诱骗行为都不能得逞。
- 另外，用户还应该注意以下几点：
  - 确认对方身份
  - 慎重对待个人信息
  - 谨防电子邮件泄密
  - 注意网站的URL地址

主要内容

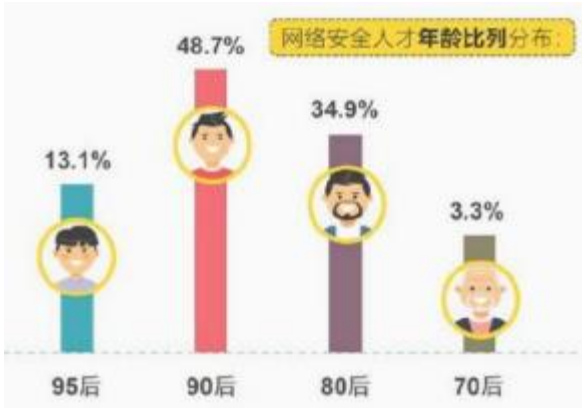
6.1 网络威胁概述
6.2 计算机病毒
6.3 网络入侵
6.4 诱骗类威胁
6.5 夺旗赛CTF

6.5.1 夺旗赛CTF

- **夺旗赛CTF（Capture The Flag）**
  - 1996年，起源于DEFCON全球黑客大会；
  - CTF竞赛取代黑客的真实攻击比拼的方式：黑客技术的赛场。
- **知名战队**
  - 美国PPP 卡耐基梅隆大学
  - 俄罗斯LC↓BC
  - 蓝莲花blue lotus

6.5.2 CTF的意义

1. 网络安全从业者经验、技术交流的重要平台;
2. 通过竞赛可以发现真实系统的漏洞，意义重大;
3. 深入理解编程、系统与安全，
4. 发现和培养网络安全人才的重要途径，建立网安人才储备;



6.5.3 竞赛模式

一、解题模式（Jeopardy）

- 以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。

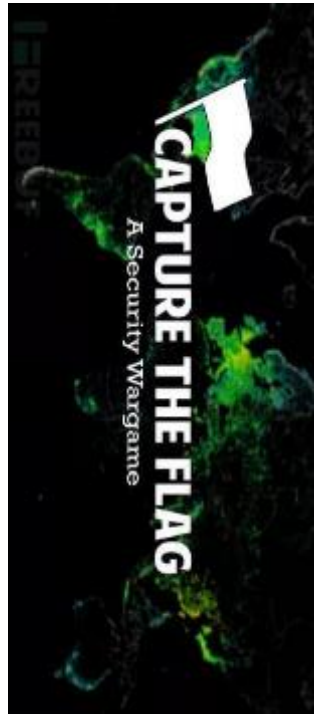
二、攻防模式（Attack-Defense）

- 在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

三、混合模式（Mix）

- 结合了解题模式与攻防模式的CTF赛制

6.5.4 竞赛题型



- **Web**：CTF夺旗竞赛中主要的题型，涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码执行、上传等漏洞
- **Crypto**：Crypto即密码学，题目考察各种加解密技术，包括古典加密技术、现代加解密技术甚至出题者自创加密技术。
- **Reverse**：Reverse即逆向工程，涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。
- **PWN**：PWN在黑客中代表攻破，取得权限，CTF比赛中代表着溢出类题目，其中常见类型溢出漏洞有栈溢出，堆溢出
- **MISC**

6.5.5一道简单的WEB题

Thanks!