信息安全导论

第七讲 网络安全技术

第七讲 网络威胁基础知识>主要内容

1. 网络攻击
2. 网络探测
3. 网络监听
4. 网络欺骗
5. 拒绝服务攻击
6. 缓冲区溢出攻击
7. SQL注入攻击
8. 计算机病毒及恶意软件

网络威胁

网络系统普遍存在的脆弱性导致网络安全面临的风险，其发展大致经历了三个阶段。

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、军事、政治利益为目的。

目前的网络威胁往往是集多种特征于一体的混合型威胁。

安全漏洞概念（略）

安全漏洞按其对目标主机的危险程度一般分为三级：

1、A级漏洞

它是允许恶意入侵者访问并可能会破坏整个目标系统的漏洞。威胁最大，系统级管理配置错误，远程访问软件常见。

2、B级漏洞

它是允许本地用户提高访问权限，并可能允许其获得系统控制的漏洞。本地用户越权访问，缓冲区溢出被利用。

3、C级漏洞

它是任何允许用户中断、降低或阻碍系统操作的漏洞。**DDOS**等。

攻击的一般流程：攻击者在实施网络攻击时的一般流程包括几个步骤：信息的收集、系统安全缺陷探测、实施攻击和巩固攻击成果四个阶段。

1、信息的收集：攻击者选取攻击目标主机后，利用公开的协议或工具通过网络收集目标主机相关信息的过程。

2、系统安全缺陷探测：在收集到攻击目标的相关信息后，攻击者通常会利用一些自行编制或特定的软件探测攻击目标，寻找攻击目标系统内部的安全漏洞，为实施真正的攻击做准备。

3、实施攻击：当获取到足够的信息后，攻击者就可以结合自身的水平及经验总结制定出相应的攻击方法，实施真正的网络攻击。

4、巩固攻击成果：在成功实施攻击后，攻击者往往会利用获取到的目标主机的控制权，清除系统中的日志记录和留下后门。

除了这四个基本的攻击步骤外，高明的攻击者往往会在实施攻击前做好自身的隐藏工作，以规避被网络安全技术人员追踪的风险。

- 网络攻击的分类

网络攻击在较高的层次上可分为两类：主动攻击和被动攻击

1. 主动攻击：指攻击者访问他所需信息必须要实施其主观上的故意行为。主动攻击包括拒绝服务攻击、信息篡改、资源使用、欺骗等攻击方法。

2. 被动攻击：主要是收集信息而不是进行访问，数据的合法用户很难觉察到这种攻击行为。被动攻击包括嗅探、信息收集等攻击方法。

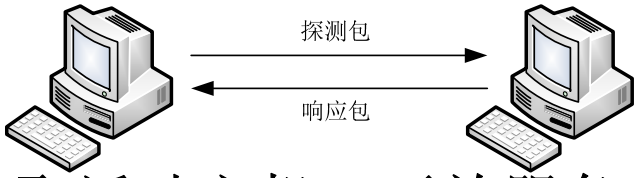
攻击者在实施网络攻击时一般都会综合运用主动和被动攻击技术，以下将详细介绍各种常见的攻击技术。

由于初始信息的未知性，网络攻击通常具备一定的难度。因此，探测是攻击者在攻击开始前必需的情报收集工作。

1. 网络踩点

指攻击者收集攻击目标相关信息的方法和步骤。发现漏洞、寻找薄弱环节、确定攻击时机等，目标：名字、邮件地址、IP地址范围、DNS服务器、邮件服务器等相关信息。

2. 网路扫描



攻击者获取活动主机、开放服务、操作系统、安全漏洞等关键信息的重要技术。扫描技术包括Ping 扫描（确定哪些主机正在活动）、端口扫描（确定有哪些开放服务）、操作系统辨识（确定目标主机的操作系统类型）和安全漏洞扫描（获得目标上存在着哪些可利用的安全漏洞）。

1、TCP 连接扫描：争取与目标主机握手，易被目标发现。

2、TCP SYN 扫描：“半连接”扫描，如返回SYN/ACK，等待连接状态；如收到RST/ACK应答，则端口未开放，比较隐蔽。

3、TCP FIN扫描：扫描工具向目的端口发送FIN请求，如端口关闭，按照RFC793的要求，应该返回RST包。适用于UNIX 系统主机，WINDOWS系统（没有遵守RFC793）不受影响。

4、TCP ACK 扫描：向目标端口发送ACK包，可以用来检测“防火墙”安装情况。了解防火墙类型等信息。

5、TCP 窗口扫描：根据返回包的窗口值，检测目标系统端口是否开放、是否过滤。

6、TCP RPC 扫描：用于UNIX系统，检查远程过程调用的端口以及对应的应用程序及其版本等信息。

7、UDP 扫描：向目标端口发送UDP包，如返回“ICMP PORT UNREACHABLE”，则端口关闭；否则端口开放。

8、ICMP协议扫描：通过向目的主机发送ICMP探测包，分析应答包数据可以探测目的主机操作系统类型等信息。ICMP探测包和正常数据包类似，入侵检测难以发现。

3. 网络查点

攻击者常采用的从目标系统中抽取有效账号或导出资源名的技术。通常这种探测方式是通过主动同目标系统建立连接来获取信息，因此这种探测方式在本质上要比网络踩点和网络扫描更具有入侵效果。查点技术通常收集的信息包括用户名、组名、系统类型、路由表信息等。

a)视频植入木马

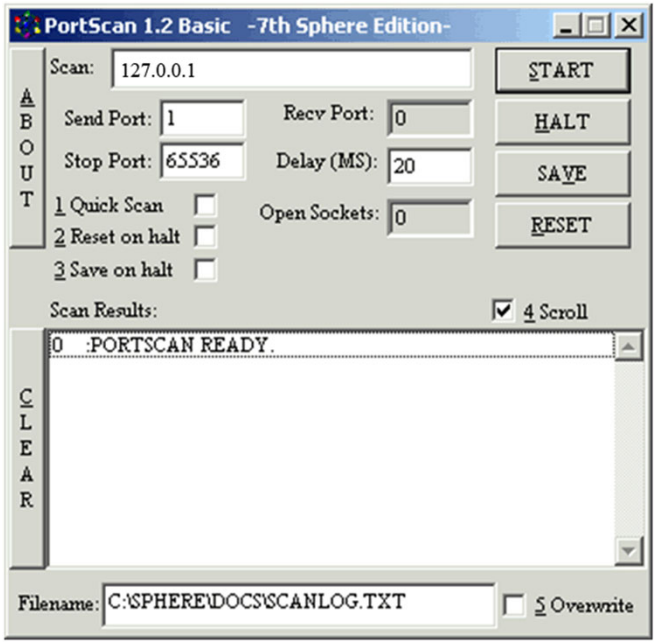
b)查找黑客最新漏洞公告，先于补丁发布进行攻击

c)社会工程学

常见扫描工具

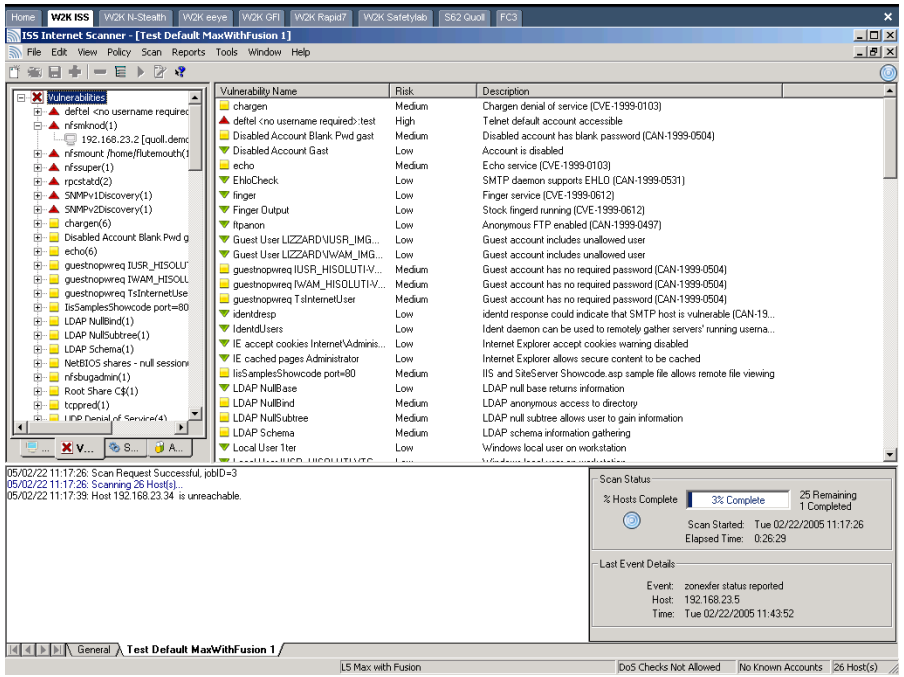
Nmap（Network Mapper）：Linux下的网络扫描和嗅探工具包。其基本功能有三个：探测主机是否在线；扫描主机端口，嗅探所提供的网络服务；推断主机所用的操作系统。

PortScan： 端口扫描小工具，可以用于扫描目的主机的开放端口，并探测其操作系统。支持Edge、Wi-Fi和3G网络。其运行界面如图所示。



Nessus 具有扫描任意端口任意服务的能力；以用户指定的格式（**ASCII**文本、**html**等）产生详细的输出报告，包括目标的脆弱点、怎样修补漏洞以防止攻击者入侵及危险级别。

ISS Internet Scanner：是**ISS**公司推出的商业安全扫描产品之一。其包括三个组件：**Intranet Scanner**，**Firewall Scanner**，**Web Server Scanner**，可以对**UNIX**和**WINNT**系统的网络通讯服务、操作系统和关键应用程序进行有计划和可选择的检测，自动扫描所连接的主机、防火墙、**Web**服务器和路由器等设备，生成详细的技术报告或高度概括的管理级报告，协助管理人员进行网络安全审计，并提供软件生产商修补其产品安全漏洞的补丁程序发布站点的链接。



指攻击者通过非法手段对系统获得监视从而获得一些关键安全信息的技术手段。

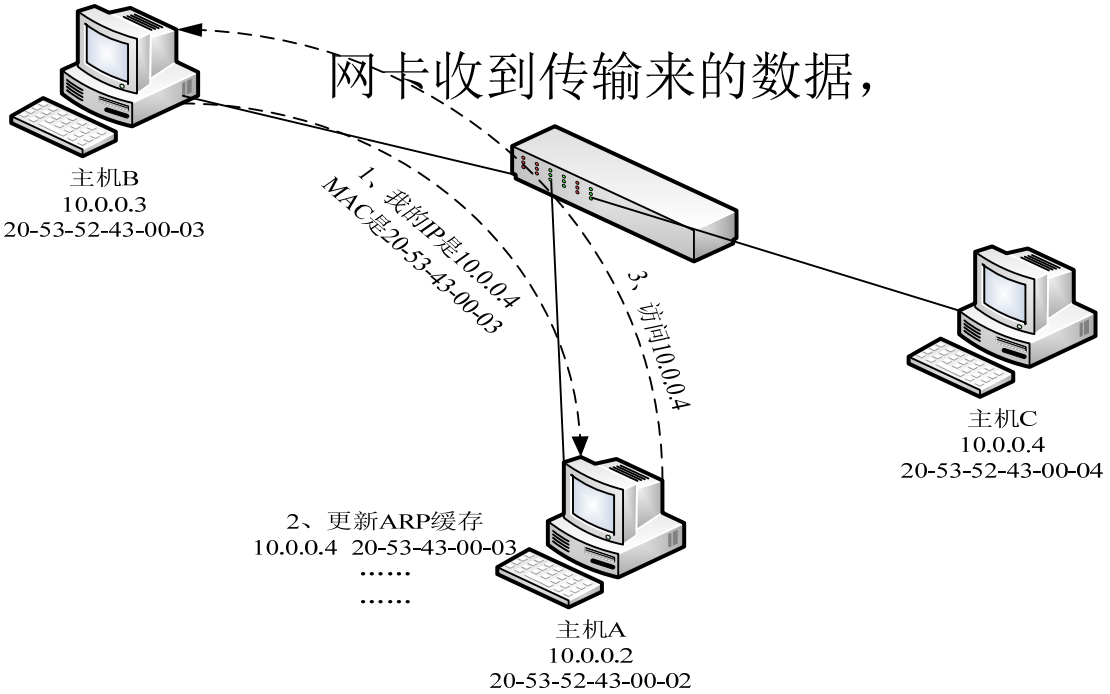
工作原理：

网卡收到传输来的数据，网卡的驱动程序先接收数据头的目标MAC地址，根据主机上的网卡驱动程序配置的接收模式判断是否接收。在默认状态下网卡只把发给本机的数据包（包括广播数据包）传递给上层程序，其它的数据包一律丢弃。

但是网卡可以设置为一种特殊的工作方式——混杂模式（Promiscuous Mode），在这种状态下，网卡将把接收到的所有数据包都传递给上层程序，这时，上层应用程序就能够获取本网段内发往其他主机的数据包，从而实现了对网络数据的监听。能实现网络监听的软件通常被称为嗅探（Sniffer）工具。

- 易： 在共享环境下，因为所有数据包的发送都是以广播的形式进行，因此只需简单地将网卡设为混杂模式，就可以捕获网络上传输的所有数据包。

- 难：在交换环境下，因为数据包的发送是由交换机进行定向转发，因此必须扰乱交换机的定向转发机制，将本该发往其他主机的数据包转发到本地主机上才能实现网络监听。



交换环境下ARP欺骗

网络监听的基本检测方法主要有：

1、用正确的IP地址和错误的MAC地址ping可疑的主机，运行监听程序的主机可能会有响应。

2、向网上发大量不存在的MAC地址的包，由于监听程序要分析和处理大量的数据包会占用很多的CPU资源，这将导致性能下降。通过比较前后该主机性能加以判断。这种方法需要获取主机的实时运行状态，因此难度较大；

3、使用反监听工具如Antisniffer，TripWare等检测工具进行检测，这些软件主要通过分析网络异常来判断是否存在嗅探器，往往对使用者有比较高的要求。

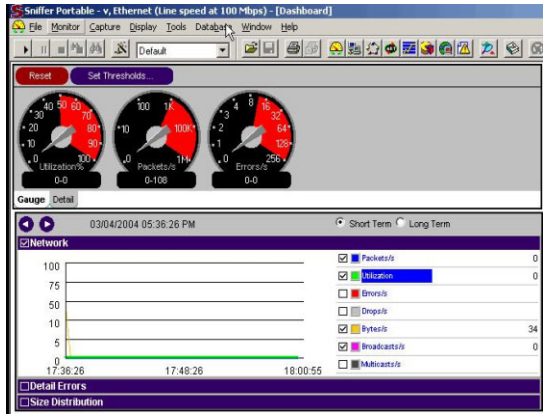
主要防范措施包括：

1、从逻辑或物理上对网络分段；

2、以交换式集线器代替共享式集线器；

3、使用加密技术；

4、划分虚拟局域网（VLAN）运用VLAN技术，将以太网通信变为点到点通信



Sniffer Pro

网络监听工具：Sniffer Pro、Ethereal、Libpcap/WinPcap、Iris等

常见的网络欺骗包括：IP源地址欺骗、DNS欺骗和源路由选择欺骗。

IP源地址欺骗就是伪造某台主机的IP地址的技术。通过IP地址的伪造使得某台主机能够伪装成另外一台主机，而这台主机往往具有某种特权或者被另外的主机所信任。

IP源地址欺骗过程主要包含5个步骤：

- 1）选定目标主机A；
- 2）发现信任模式及受信任主机B；
- 3）使主机B丧失工作能力；
- 4）伪装成主机B向主机A发送建立TCP连接请求，并猜测主机A希望的确认序列号；
- 5）用猜测的确认序列号发送确认信息，建立连接。

防范对策：

1）不使用基于地址的信任策略，使用更安全的通信手段，如SSH；

2）使用包过滤；边界路由器包过滤，只有内部网络采用IP信任，来自外部网络的源和目的都是内部网络时，被攻击了。。。

3）使用加密机制。

DNS欺骗

在DNS报文中只使用一个序列号来进行有效性鉴别，未提供其它的认证和保护手段，这使得攻击者可以很容易地监听到查询请求，并伪造DNS应答包给请求DNS服务的客户端，从而进行DNS欺骗攻击。如被骗访问伪造网站。

防范：合法应答包信息全面，非法包为了抢先生成通常不包含授权域和附加域。
1）加权法；根据数据包情况计算最终可信度，最后选择可信度最高的应答包。
2）贝叶斯分类法；设计一个两类贝叶斯分类器来区分合法和欺骗包。
3）交叉验证法；收到应答后向DNS服务器反向查询。

源路由选择欺骗

在通常的TCP数据包中只包括源地址和目的地址，即路由只需知道一个数据包是从哪来的要到哪去。源路由是指在数据包首部中列出了所要经过的路由。某些路由器对源路由包的反应是使用其指定的路由，并使用其反向路由来传送应答数据。这种攻击称为源路由选择欺骗（Source Routing Spoofing）。

伪装信任用户向攻击目标发源路由数据包。

防范方法：

1）杜绝IP源地址欺骗；

2）关闭路由器源路由功能。

理解

拒绝服务攻击

- 拒绝服务攻击DoS (Denial of Service)，设法使目标主机停止提供服务，耗尽目标通信、存储或计算资源，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
- 分布式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

1、SYN泛洪，使被攻击主机的资源耗尽（CPU满负荷或内存不足），而停止服务。其攻击过程如图所示。

Syn Flood攻击

正常的三次握手建立通讯的过程

2、UDP泛洪

攻击者利用简单的TCP/IP服务，如字符发生器协议（Chargen）和Echo来传送占满带宽的垃圾数据。

3、Ping泛洪

由于在早期的阶段，路由器对包的最大尺寸都有限制。许多操作系统对TCP/IP堆栈的实现在ICMP包上都是规定64KB，当声称自己的尺寸超过ICMP上限的包也就是加载的尺寸超过64KB上限时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接受方主机宕机。

4、泪滴攻击

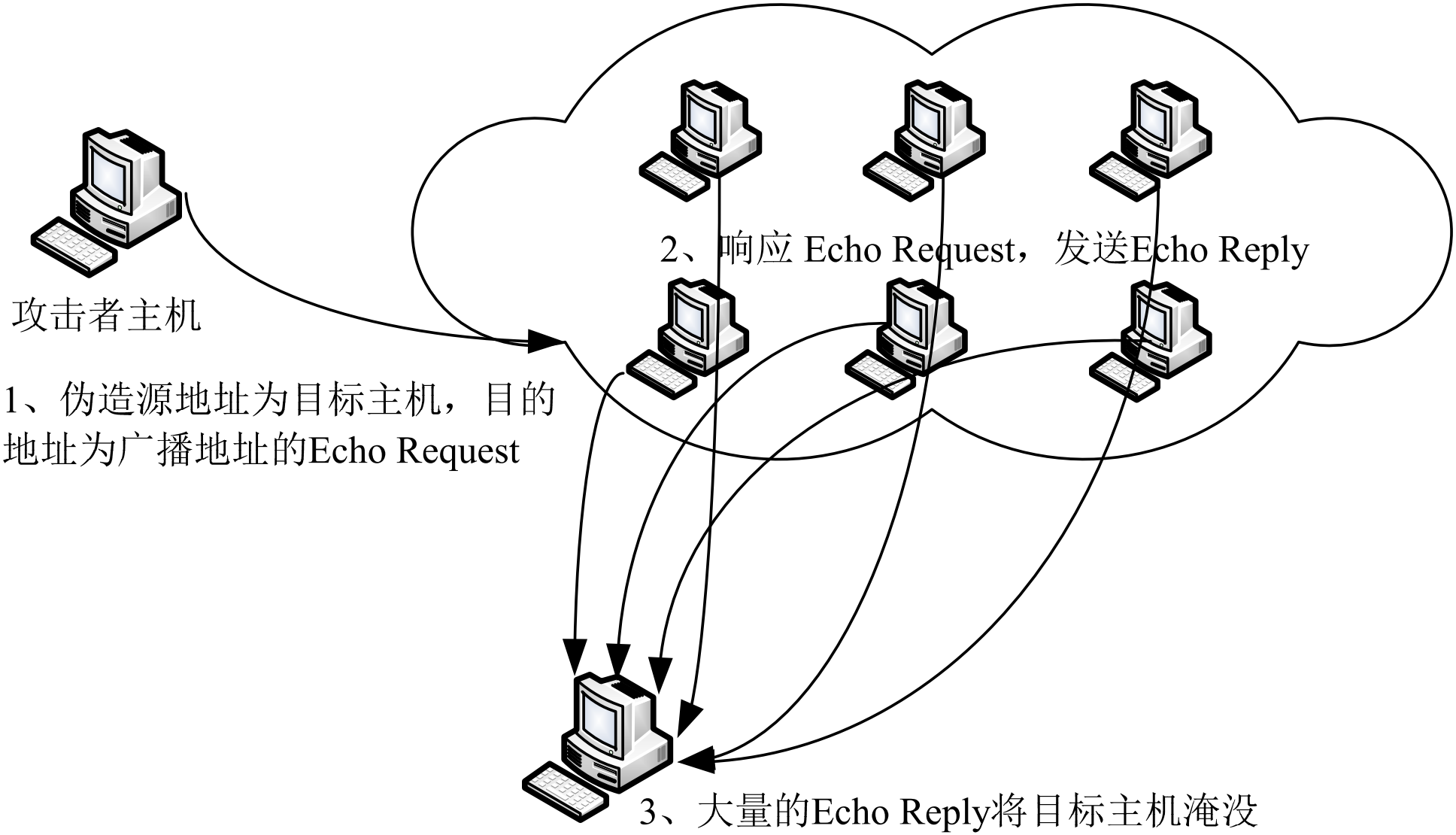
泪滴（teardrop）攻击是利用在TCP/IP堆栈中实现信任IP碎片中的包的标题头所包含的信息来实现自己的攻击。IP分段含有指明该分段所包含的是原包的哪一段的信息，某些TCP/IP（包括Service Pack 4以前的WINNT）在收到含有重叠偏移的伪造分段时将崩溃。

5、Land攻击

设计一个特殊的SYN包，它的原地址和目标地址都被设置成某一个服务器地址。

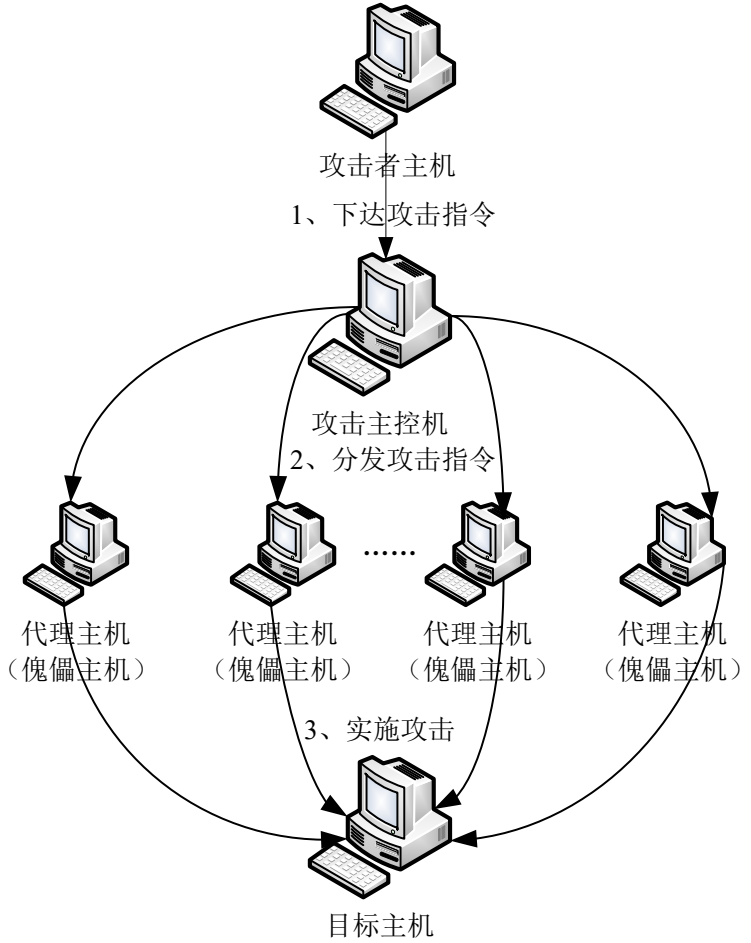
6、Smurf攻击

软件Smurf得名，通过广播地址发出ICMP回应请求，回复设为攻击目标。反弹攻击


攻击者主机
1、伪造源地址为目标主机，目的地址为广播地址的Echo Request
2、响应 Echo Request，发送Echo Reply
3、大量的Echo Reply将目标主机淹没目标主机

分布式拒绝服务攻击（DDoS）

借助于客户/服务器技术，将多台主机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个主控程序控制预先被植入到大量傀儡主机中的代理程序。代理程序收到特定指令时就同时发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行，因此能够产生比DoS攻击更大的危害后果，其攻击过程如图所示。



拒绝服务攻击防范：

1、主机设置

1）关闭不必要的服务；
2）限制同时打开的SYN半连接数目；
3）缩短SYN半连接的超时等待（Time Out）时间；
4）及时更新系统补丁。

2、防火墙和路由器设置

防火墙：

1）禁止对主机的非开放服务的访问；

2）限制同时打开的SYN最大连接数；

3）限制特定IP地址的访问；

4）启用防火墙的防DoS/DDoS的属性；

5）严格限制对外开放的服务器的向外访问，这主要是防止服务器被攻击者利用。

路由器设置：

1）使用扩展访问列表，扩展访问列表是防止DoS/DDoS攻击的有效工具。

2）使用QoS，

3）使用单一地址逆向转发，

4）使用TCP拦截，Cisco公司的路由器在IOS 11.3版以后，引入了TCP拦截功能，这项功能可以有效防止SYN Flood攻击内部主机。

5）使用基于内容的访问控制

缓冲区溢出攻击（Buffer Overflow）是利用缓冲区溢出漏洞所进行的攻击行动。缓冲区溢出是一种非常普遍、非常危险的漏洞，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，可以导致序运行失败、系统关机、重新启动等后果，精心设计的缓冲区溢出攻击甚至可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。

缓冲区溢出的基本原理是：攻击者通过向目标程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如下面程序：

```
void function(char *in)
{
char buffer[128];
strcpy(buffer, in);
}
```

当字符串in的长度大于128，就会造成缓冲区溢出！

缓冲区溢出漏洞在很多软件中都存在，根据计算机应急响应小组（CERT）的统计，超过50%的安全漏洞都是缓冲区溢出造成的，“红色代码”、“冲击波”、“Slammer蠕虫”等恶意代码均是利用不同的缓冲区溢出漏洞进行传播和实施攻击的。

缓冲区溢出的防范

1）通过操作系统控制使接收输入数据的缓冲区不可执行，从而阻止攻击者植入攻击代码；

2）要求程序员编写正确的代码，包括严格检查数据，不使用存在溢出风险的函数，利用Fault Injection等工具进行代码检查等；

3）利用编译器的边界检查来实现缓冲区的保护，这个方法使得缓冲区溢出不可能出现，从而完全消除了缓冲区溢出的威胁，但是相对而言代价比较大。

结构化查询语言（Structured Query Language，SQL）是一种用来和数据库交互的文本语言，SQL注入攻击（SQL Injection）就是利用某些数据库的外部接口把用户数据插入到实际的数据库操作语言当中，从而达到入侵数据库乃至操作系统的目的。

在Web应用程序的登录验证程序中，一般有用户名（username）和密码（password）两个参数，程序会通过用户所提交输入的用户名和密码来执行授权操作。其原理是通过查找user表中的用户名（username）和密码（password）的结果来进行授权访问，典型的SQL查询语句为：

Select * from users where username= ‘Bob’ and password= ‘helloworld’

如果分别给username和password赋值“admin’ or 1=1—”和“aaa”。那么，SQL脚本解释器中的上述语句就会变为：

Select * from users where username= ‘admin’ or 1=1—and password= ‘aaa’

SQL注入步骤：

1、寻找SQL注入点；

2、获取和验证SQL注入点；

3、获取信息：获取信息是SQL注入中一个关键的部分，SQL注入中首先需要判断存在注入点的数据库是否支持多句查询、子查询、数据库用户账号、数据库用户权限。

4、实施直接控制；

5、间接进行控制：间接控制主要是指通过SQL注入点不能执行命令，只能进行数据字段内容的猜测。

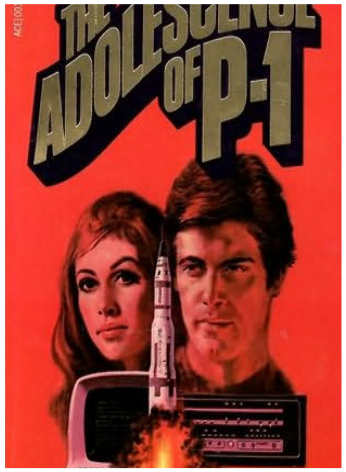
SQL注入攻击针对的是应用开发过程中的编程缺陷，防范只能从代码检查抓起。

计算机病毒的起源

冯.诺伊曼

1949年在论文《复杂自动装置的理论及组织的进行》里，已经勾勒出病毒程序的蓝图。他指出存在可以自我复制的程序。

托马斯·丁·雷恩



1977年在科幻小说《Adolescence of P-1》中，描写了一种可以在计算机中互相传染的病毒。

弗雷德·科恩

1983年，弗雷德·科恩在南加州大学写出了第一个可自我复制并具有感染能力的程序。

计算机病毒定义

课本：计算机病毒是一种人为制造的、在计算机运行中对计算机信息或系统起破坏作用的程序。

计算机病毒的狭义定义

- 计算机病毒是一种靠修改其它程序来插入或进行自身拷贝，从而感染其它程序的一种程序。—— Fred Cohen博士

我国的计算机病毒定义

- 《中华人民共和国计算机信息系统安全保护条例》第二十八条："计算机病毒，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毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机病毒的广义定义

- 能够引起计算机故障，破坏计算机数据，影响计算机系统的正常使用的程序代码

记忆

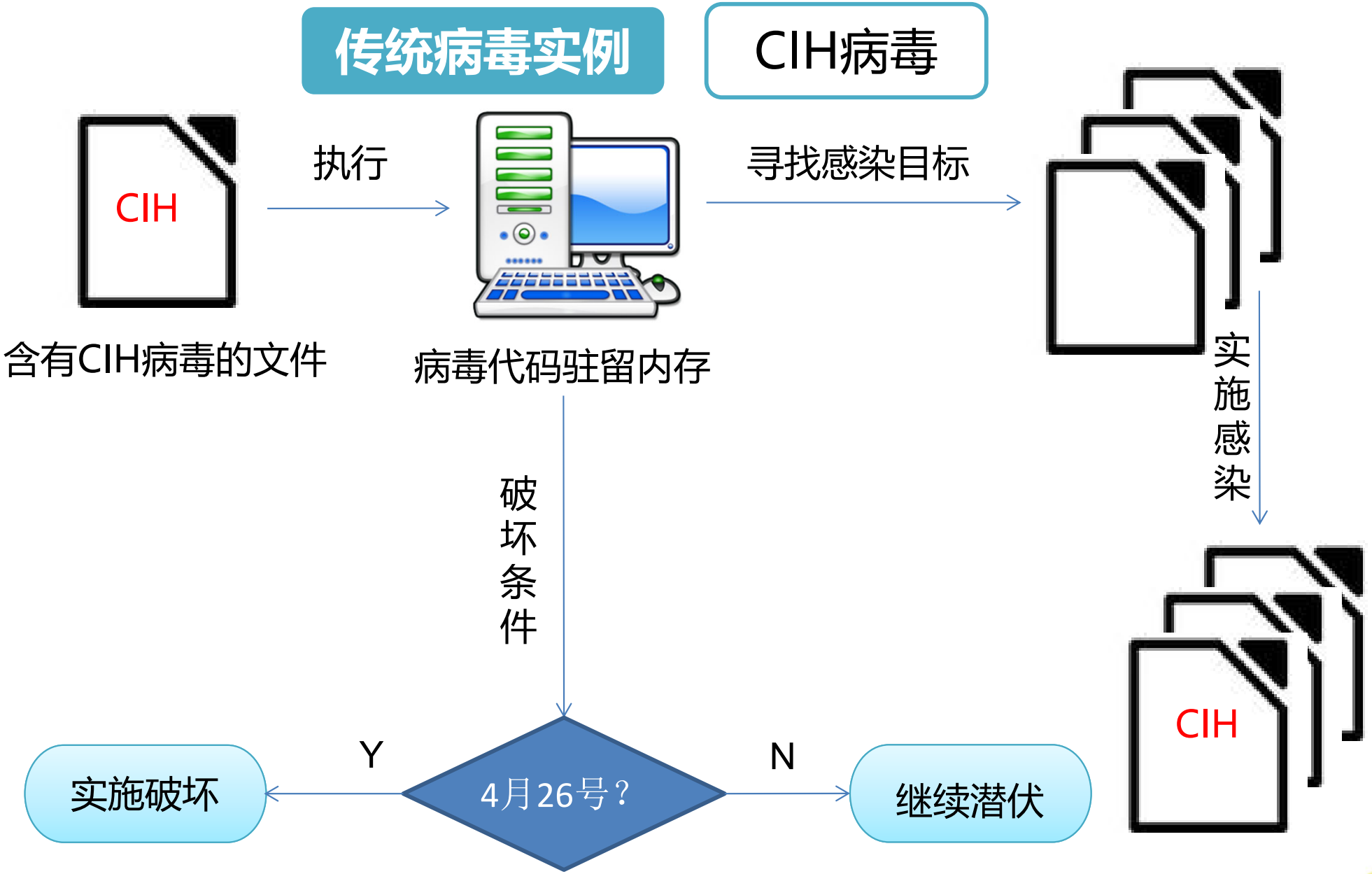
计算机病毒特征和发展趋势

记忆 **计算机病毒的分类**

一、传统病毒

传统病毒传统型计算机病毒的共同特色，就是一定有一个「宿主」程序，所谓宿主程序就是指那些让计算机病毒藏身的地方。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。

- 引导型病毒：隐藏在磁盘的引导区中，小球、大麻、米开朗琪罗
- 文件型病毒：隐藏在可执行文件（COM，EXE）1575、中国炸弹、CIH
- 宏病毒：隐藏在Office文档或模板的宏中，Nuclear、台湾1号


传统病毒实例
CIH病毒
CIH
执行
寻找感染目标
含有CIH病毒的文件
病毒代码驻留内存
实施感染
破坏条件
CIH
Y
N
实施破坏
4月26号？
继续潜伏

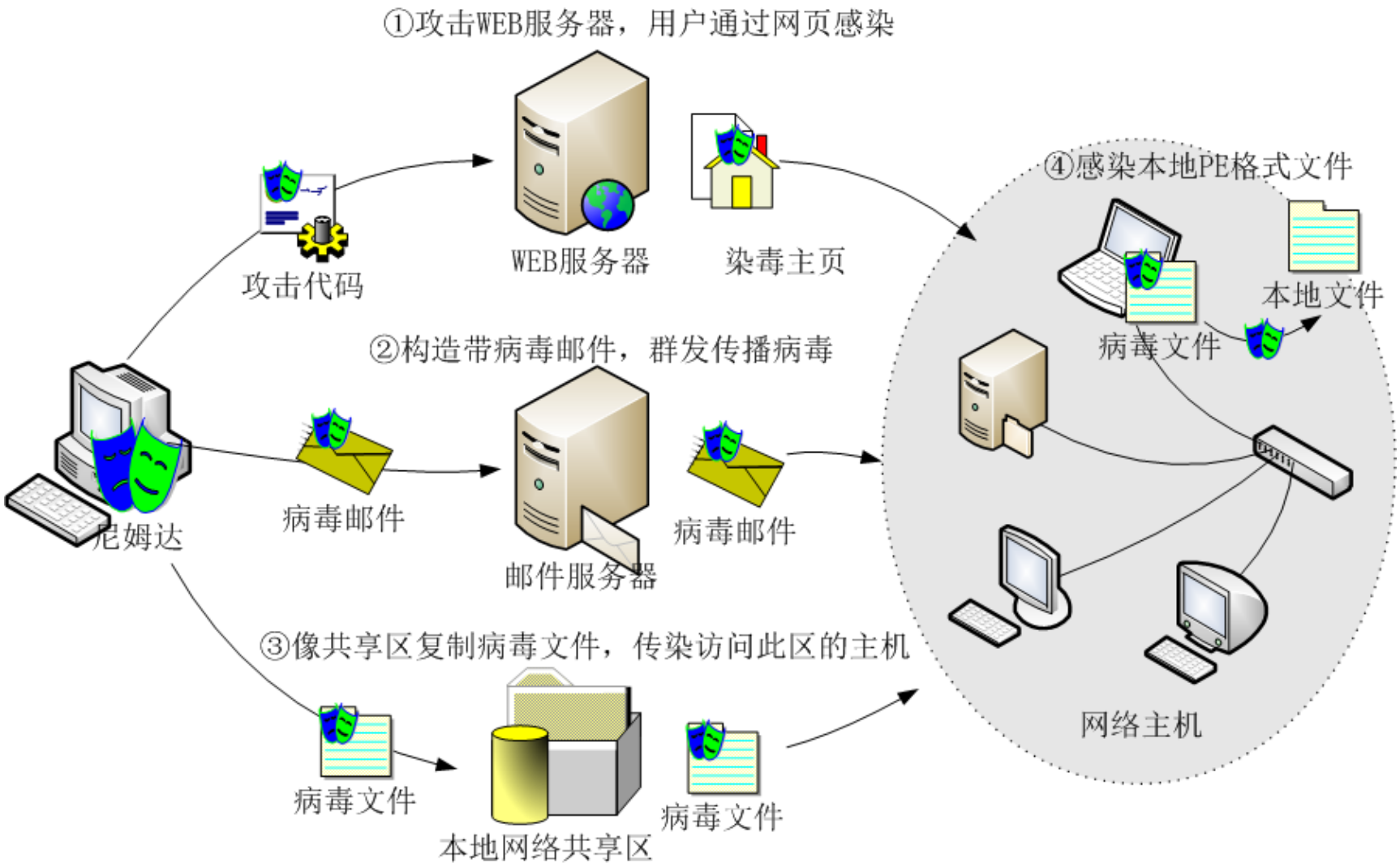
记忆 **计算机病毒的分类**

二、蠕虫病毒

- 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

蠕虫病毒实例

尼姆达病毒



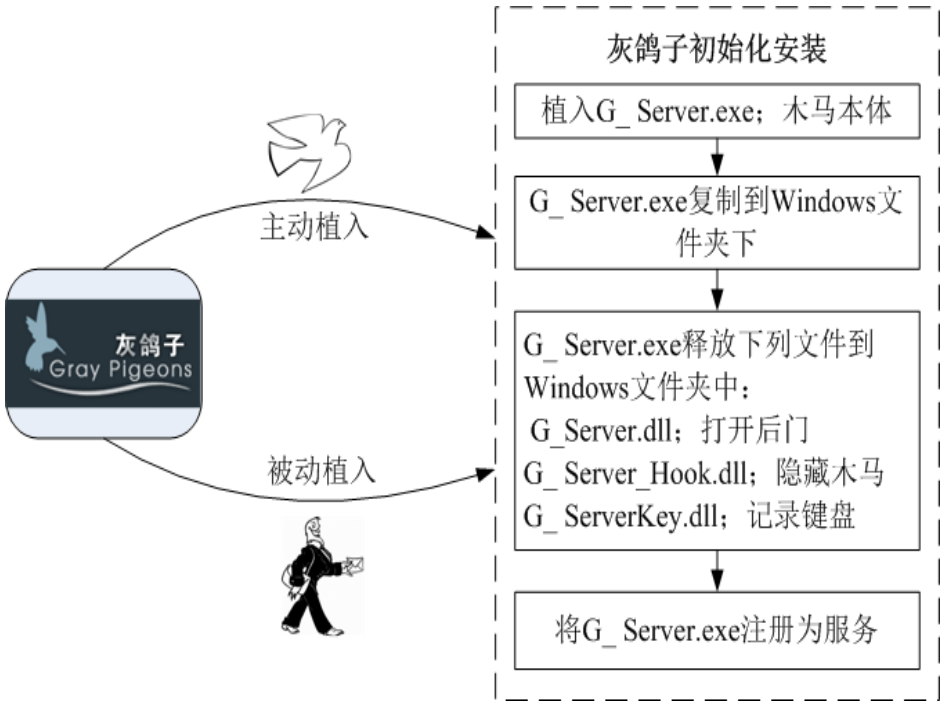
理解 **计算机病毒的分类**

三、木马病毒

- 1986年的PC-Write木马是世界上第一个计算机木马，木马一般不会直接对电脑产生危害，以控制电脑为目的；
- 木马是有隐藏性和传播性的，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；
- 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。

木马病毒实例

灰鸽子病毒



还有蜜蜂大盗（DLL木马）、冰河木马（远程控制）等

计算机病毒预防

- 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；
- 注意光盘以及U盘等存储媒介；
- 在使用光盘、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；
- 备份重要数据

本讲到此结束，谢谢聆听！

Any question?