# 第6章 网络威胁

罗文坚

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 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（Network Intrusion）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。

- 注意：对信息的非授权访问一般被称为破解（Cracking）。

- 网络入侵一般分为三个阶段：
  - 前期准备、实施入侵和后期处理。

# 网络入侵的三个阶段

- 前期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，入侵手段分为：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。

- 后期处理阶段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。

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 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。
  - 又称为业务否决攻击。

- 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

- 根据TCP/IP的规范，一个包的长度最大为65536字节。
- 但是，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，发送SYN ACK报文，回应连接请求报文，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的所有TCP缓存将被耗尽，无法向正常用户提供服务，攻击者达到了攻击的目的（拒绝服务）。

# Smurf攻击

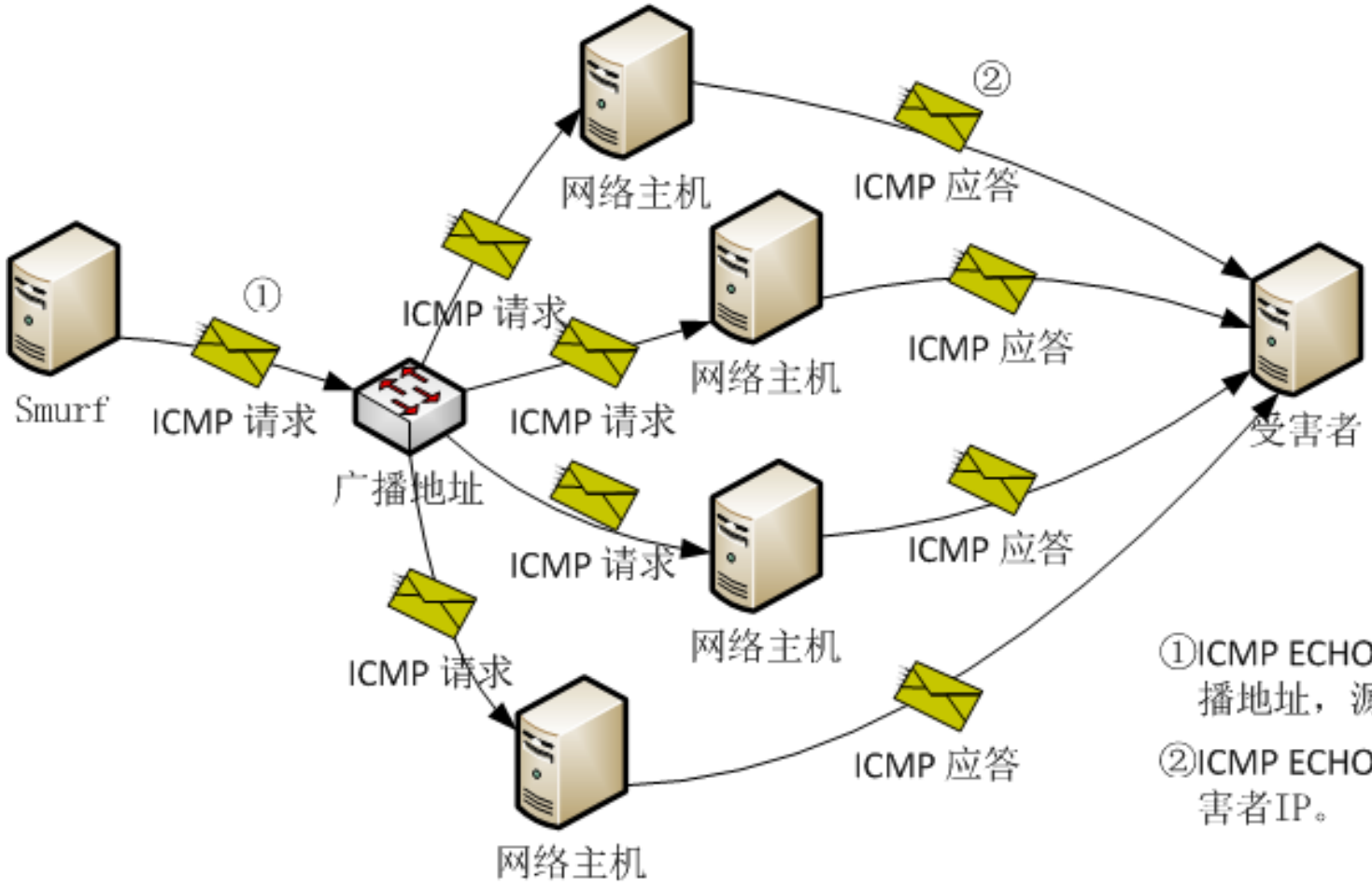
- Smurf攻击是以最初发动这种攻击的程序Smurf来命名的，这种攻击方法结合使用了IP地址欺骗和ICMP协议。

- 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，而且每个电子邮件也比较大，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。
  - 其他人发给用户的电子邮件将会丢失或者被退回，使用户的邮箱失去作用。

- 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

- 随着计算机处理能力的快速增长，内存的大量增加，以及千兆级别网络的使用，DoS攻击很难有效。
- 分布式拒绝服务攻击DDOS（Distributed Denial of Service）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攻击的防御方法

1. 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，例如，Ping of Death攻击。

2. 将主机或网络中的不必要的服务和端口关掉。
   - 例如，对于非WEB主机关掉80端口。

3. 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。

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 口令攻击步骤

- 步骤一、获取目标系统的用户帐号及其它有关信息；
- 步骤二、根据用户信息猜测用户口令；
  - 使用对于用户来说有意义的、便于记忆的数据做口令将是危险的，如用户名、用户名变形、生日、电话、电子邮件地址等。
- 步骤三、采用字典攻击方式探测口令；
- 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。

# 口令攻击步骤

- 关于获取目标系统的用户帐号及其它有关信息：一般利用一些网络服务来实现，如Finger、WHOIS、LDAP等信息服务。
- Finger是UNIX系统中用于查询用户情况的实用程序。UNIX系统保存了每个用户的详细资料，可以用Finger命令查询。
- WHOIS服务是一个在线的“请求/响应”式服务。WHOIS Server运行在后台监听43端口，当Internet用户搜索一个域名（或主机、联系人等其他信息时），WHOIS Server接收用户请求的信息并据此查询后台域名数据库。如果数据库中存在相应的记录，它会将相关信息，如所有者、管理信息以及技术联络信息等，反馈给用户。
- LDAP是轻量级目录访问协议，其目录中存放着各类信息，如Email、联系人列表等。

# 口令攻击步骤

- 关于字典攻击：
  - 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。

✓一般情况下，密码错误的连续登录次数是受限制的。

# 口令数量

- 攻击者还可能采用穷举暴力攻击的方法来攻击口令。

- 一般而言，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。

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 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。
  - 这些数据可以是网络管理员需要分析的网络流量，也可以是黑客喜欢的用户账号和密码，或者一些商用机密数据等。

- 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（也称作网络适配器或网络接口）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，就可以对在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。
- 目前，采用“共享技术”的网络设备集线器已经被采用交换方式的交换机所取代。在大多数局域网中，利用混杂模式进行监听已经不可能了。

# 交换网络环境

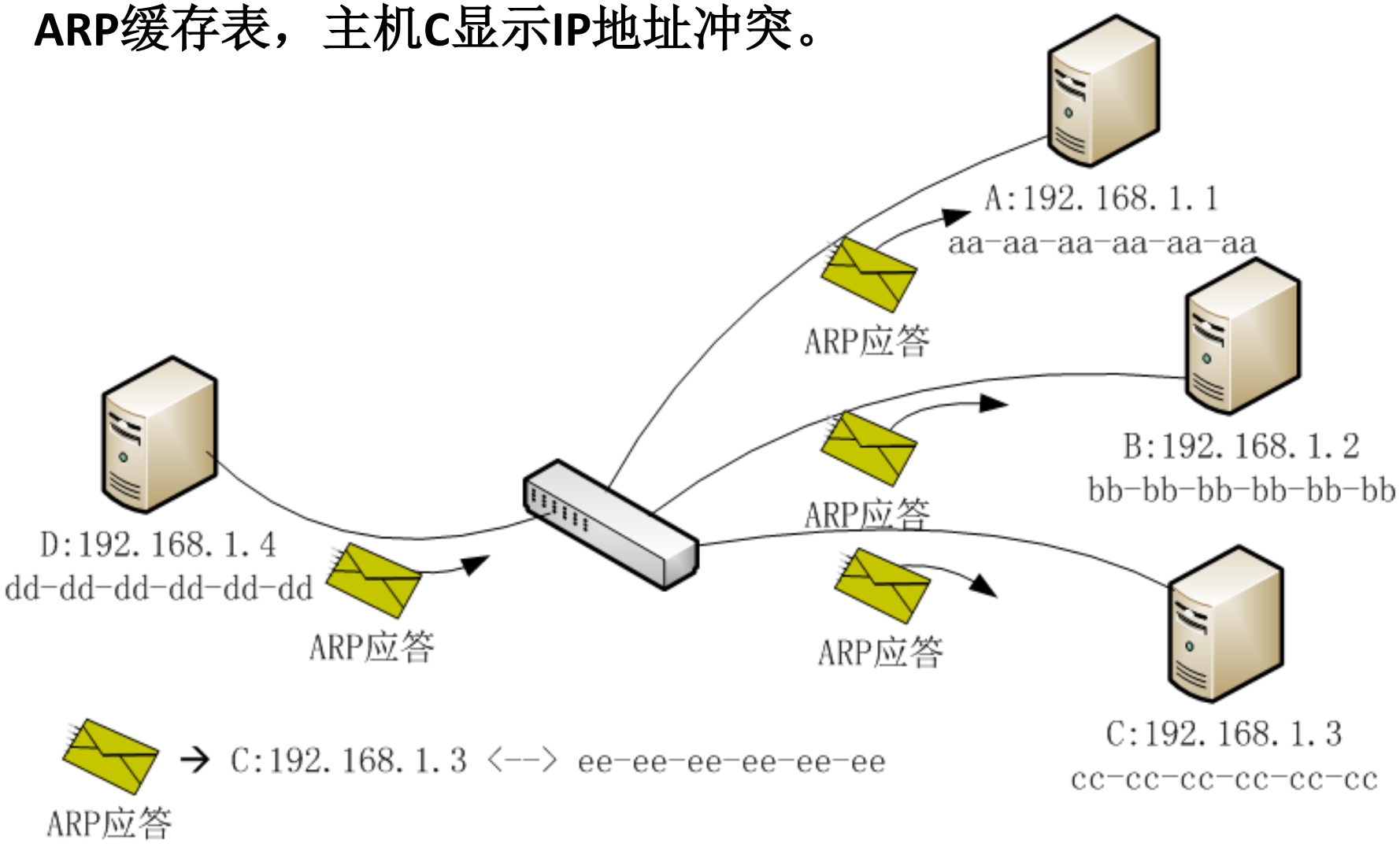
- 交换网络下的窃听是利用ARP欺骗实现的。

- ARP（Address Resolution Protocol）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协议并不只是在发送了ARP请求并接收ARP应答后，添加ARP地址缓存。

| Internet | 物理地址 | 类型 |
|---|---|---|
| 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欺骗

- 主机D给局域网中的所有主机发送ARP应答。主机A和B更新其ARP缓存表，主机C显示IP地址冲突。



# ARP欺骗

- 假设主机D想监听主机A和主机C之间的通信内容：
  - D给A发送ARP应答，告诉A，192.168.1.3主机的MAC地址是dd-dd-dd-dd-dd-dd。
  - D给C发送ARP应答，告诉C，192.168.1.1主机的MAC地址是dd-dd-dd-dd-dd-dd。

  - A想要发送给C的数据实际上发送给了D，D在嗅探到数据后将此数据转发给C。
  - C回应A的数据也发给了D，D嗅探之后转发给A。
  - 这样可以保证A和C的通信不被中断，同时达到了嗅探的目的。

# 防范嗅探攻击

- 检测嗅探器
  - 通过检测混杂模式网卡来检查嗅探器的存在，例如AntiSniff工具。
- 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。

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 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。

- 常见的假消息攻击方式：
  - IP欺骗
  - ARP欺骗
  - DNS欺骗
  - 伪造电子邮件

# 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，如SYN Flood攻击；
- 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（源IP为被目标主机信任的主机的IP地址），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。

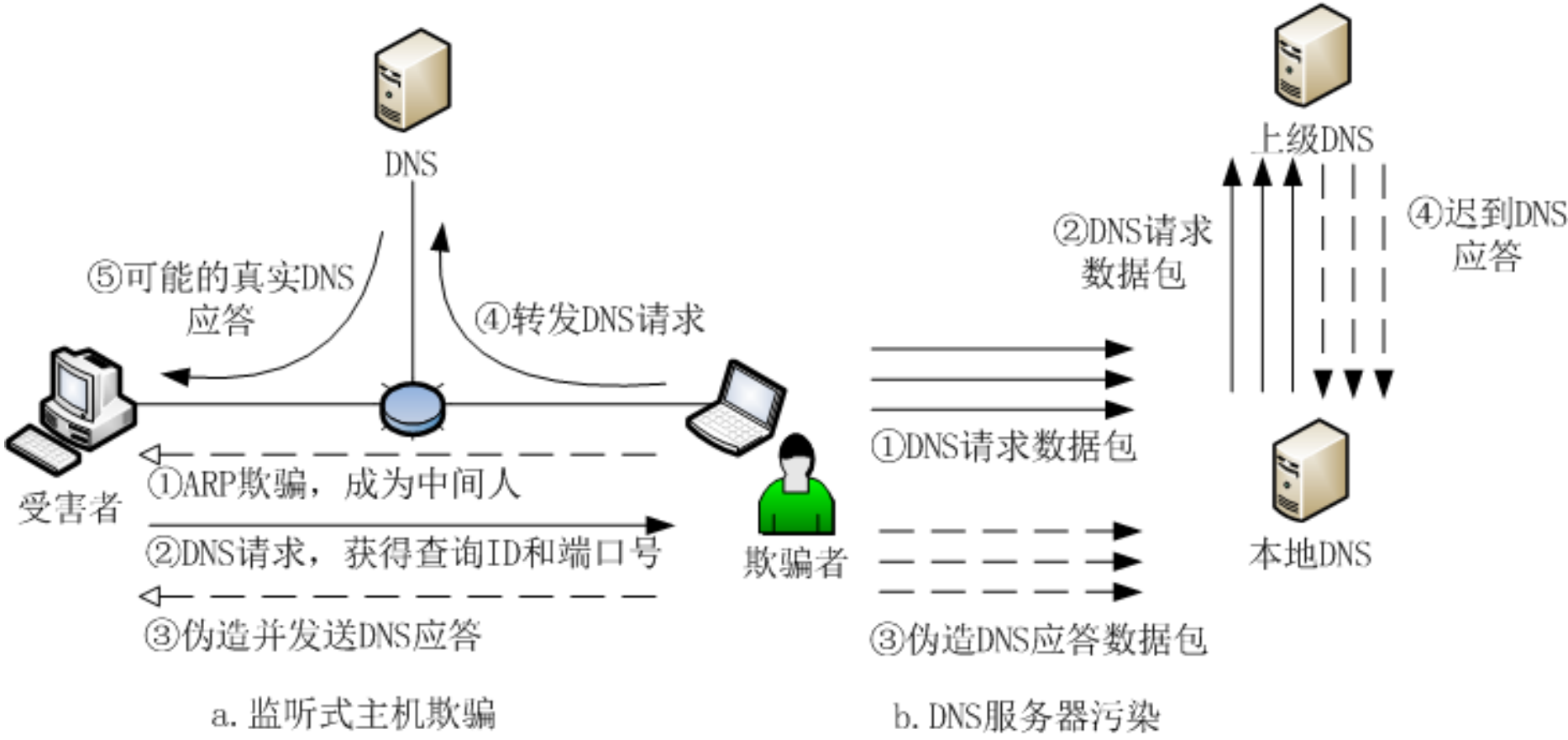
# IP欺骗攻击主要步骤

- 序列号取样和猜测：
  - 如果攻击者可以截获目标主机的SYN-ACK数据包，则可以直接计算出目标主机接收的TCP序列号，来伪造TCP数据包；
  - 否则，只能采取猜测计算的方法，攻击者先与目标主机的一个端口（如SMTP）建立起正常的连接，这个过程被重复若干次，并将目标主机的初始化系列号ISN存储起来，攻击者需要估计他的主机与被信任主机之间的往返时间RTT，然后可以预测ISN大小，并计算可能的TCP序列号。

  - ISN： Initial Sequence Number

# DNS欺骗

- DNS欺骗的目的是冒充域名服务器，把受害者要查询的域名对应的IP地址伪造成欺骗着希望的IP地址。



# 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

1. 抛弃基于地址的信任策略，不允许使用r类远程调用命令。

2. 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。

3. 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。

4. 使用PGP等安全工具并安装电子邮件证书。
   - PGP（Pretty Good Privacy，优良保密协议）是一套用于消息加密、验证的应用程序。PGP中，每个公钥均绑定唯一的用户名和/或者E-mail地址。

# 主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
  - 6.3.1 拒绝服务攻击
  - 6.3.2 口令攻击
  - 6.3.3 嗅探攻击
  - 6.3.4 欺骗类攻击
  - 6.3.5 利用型攻击
- 6.4 诱骗类威胁

# 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
  - 缓冲区溢出

# 僵尸病毒（Bot）

- 僵尸病毒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。
  - 僵尸网络常用的协议包括IRC（Internet Relay Chat）、HTTP、P2P等。

- 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（Bot）

- 僵尸病毒的传播和木马相似，传播途径包括：
  - 电子邮件；
  - 含有病毒的WEB网页；
  - 捆绑了僵尸程序的应用软件；
  - 利用系统漏洞攻击加载等。

- 黑客经常利用僵尸病毒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程序向缓冲区内填充数据位数时超过了缓冲区本身的容量时，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。

# 缓冲区溢出

- 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查，当数据被覆盖时也不能被发现。

# 缓冲区溢出

- 一般来说，缓冲区溢出漏洞是程序员写程序时的马虎所致。
- 在很多服务程序中，大意的程序员使用了像strcpy()和strcat()等不能进行有效位检查的函数。
- 攻击者利用这一问题，设计编写一些代码，并将该代码设法加载到缓冲区有效载荷末尾。
  - 这样，当发生缓冲区溢出时，返回指针指向恶意代码，从而获得系统的控制权。

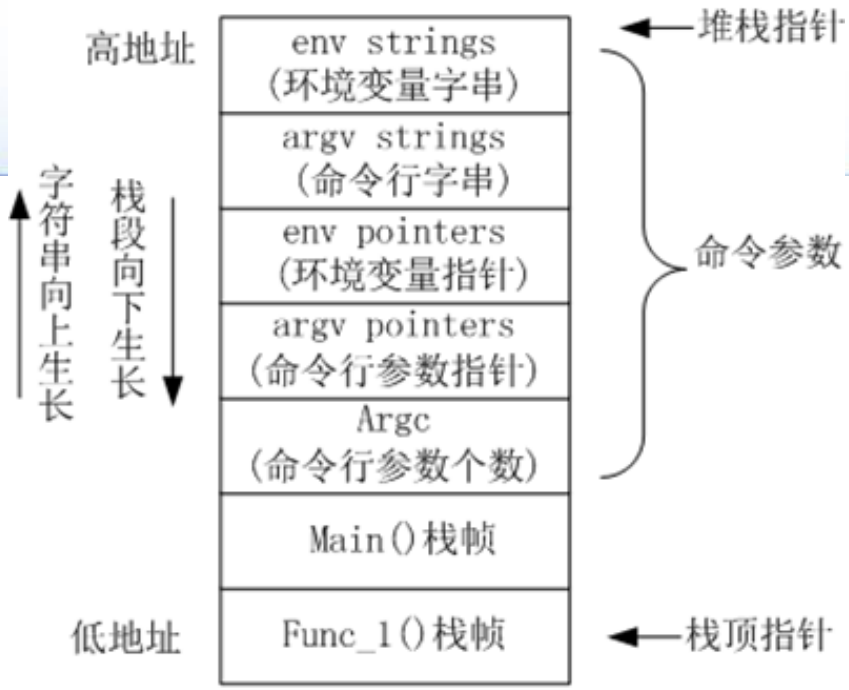
# 缓冲区溢出的例子

```
1.  #include <stdio.h>
2.  #include <string.h>
3.  void Sayhello(char* name)
4.  {
5.    char tmpName [8];
6.    strcpy(tmpName, name);
7.    printf("Hello %s\n", tmpName);
8.  }
9.  int main(int argc, char** argv)
10. {
11.   Sayhello(argv[1]);
12.   return 0;
13. }
```

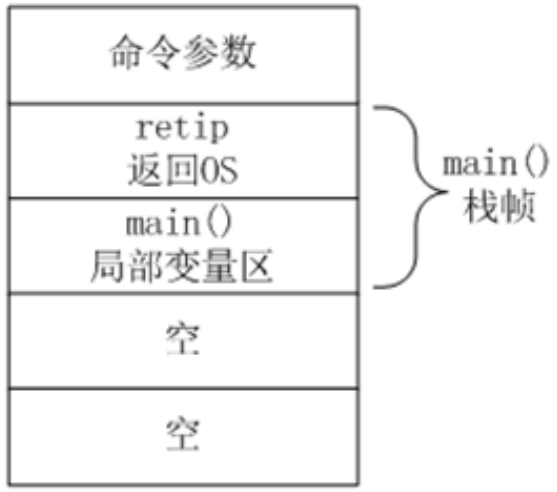
下面内容是在Linux环境下example.c程序的执行情况：

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

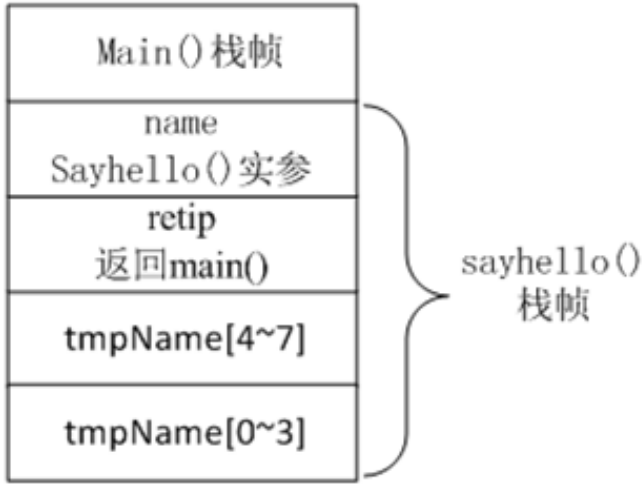
# 分析



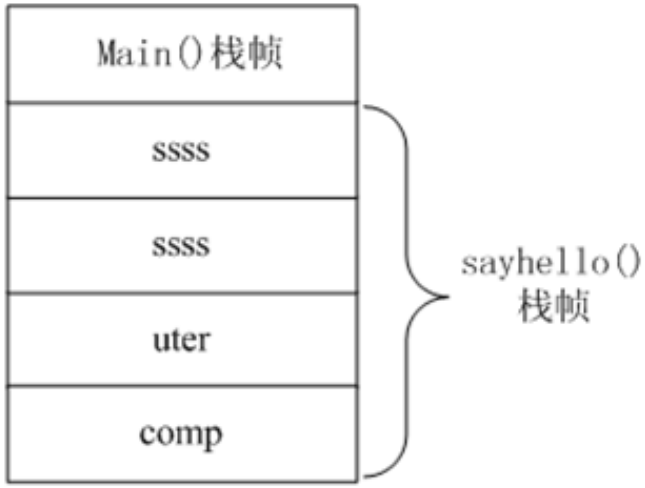

a. 程序执行时栈段分配




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

# 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。

- 例如，利用短信诈骗银行信用卡号码。

# 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。

- 电子邮件诱骗
- 假冒网站
- 虚假的电子商务

# 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，一般需要经过以下几个步骤。

1. 选定目标用户群：购买电子邮件地址；从公开的网站收集；邮件地址字典（常用名随机组合+服务提供商，例如bobsmith@gmail.com、bobsmith@163.com）。

2. 构造欺骗性电子邮件：往往包含一个容易混淆的链接，冒充受害者所信任的组织机构。

3. 搭建欺骗性网站：搭建域名和网页内容都与真正的被受害者所信任的组织机构网站极为相似的网站。

4. 群发邮件，等待上当的受害者。

# 假冒网站

- 建立假冒网站，骗取用户帐号、密码实施盗窃，这是对用户造成经济损失最大的恶劣手段。

- 攻击者建立起域名和网页内容都与真正的网上银行、网上证券交易等重要部门网站极为相似的假冒网站，并通过各种方式传播给用户。

- 例如，非法网址为“http: //www. 1cbc. com. cn”，而真正银行的网址是“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。

# 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：不要在电子邮件中泄露私人的或财务方面的信息。
  - 注意网站的URL地址。

# 作业

1. 习题2（6）：ARP欺骗的原理是什么？
2. 习题2（7）：DNS欺骗是如何实现的？
3. 不使用strcpy()函数，写一个能引起缓冲区溢出的小程序，并简要解释该程序为什么会引起缓冲区溢出。