信息安全基础

（二）网络安全
——网络攻击

刀，是基本生活用具，也是伤人凶器

- 网络信息安全技术与黑客攻击技术都源于同一技术核心，即网络协议和底层编程技术，不同的是怎么使用这些技术。
- 很多软件或设备可以为网络管理和安全提供保障，但当被别有用心的人所利用时，就成了黑客工具。

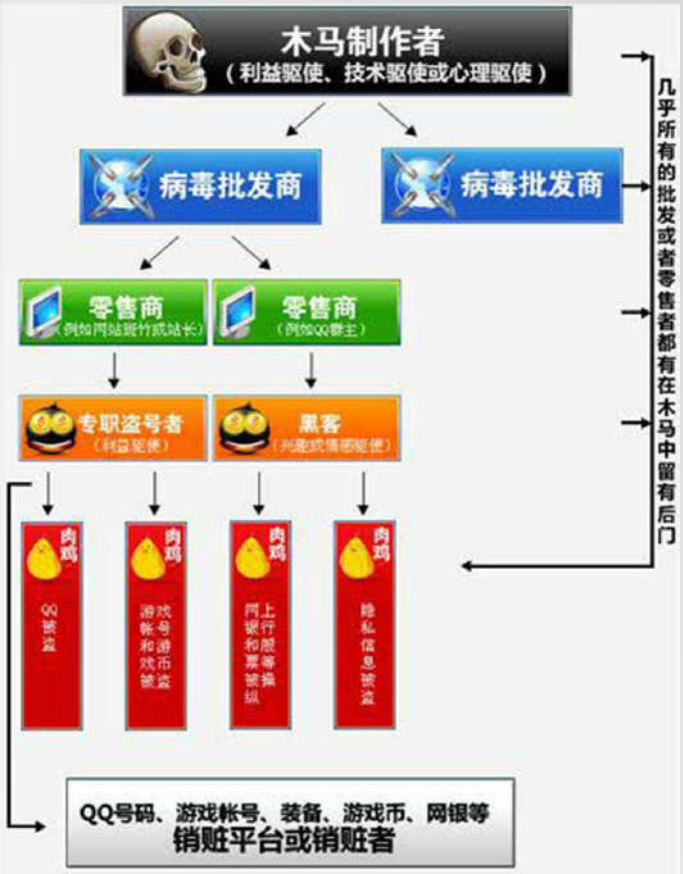
威胁的分类

- 计算机网络系统所面临的威胁大体可分为两种：一是针对网络中信息的威胁；二是针对网络中设备的威胁。
- 按威胁的对象、性质则可以细分为四类：
  - 第一类是针对硬件实体设施
  - 第二类是针对软件、数据和文档资料
  - 第三类是兼对前两者的攻击破坏
  - 第四类是计算机犯罪

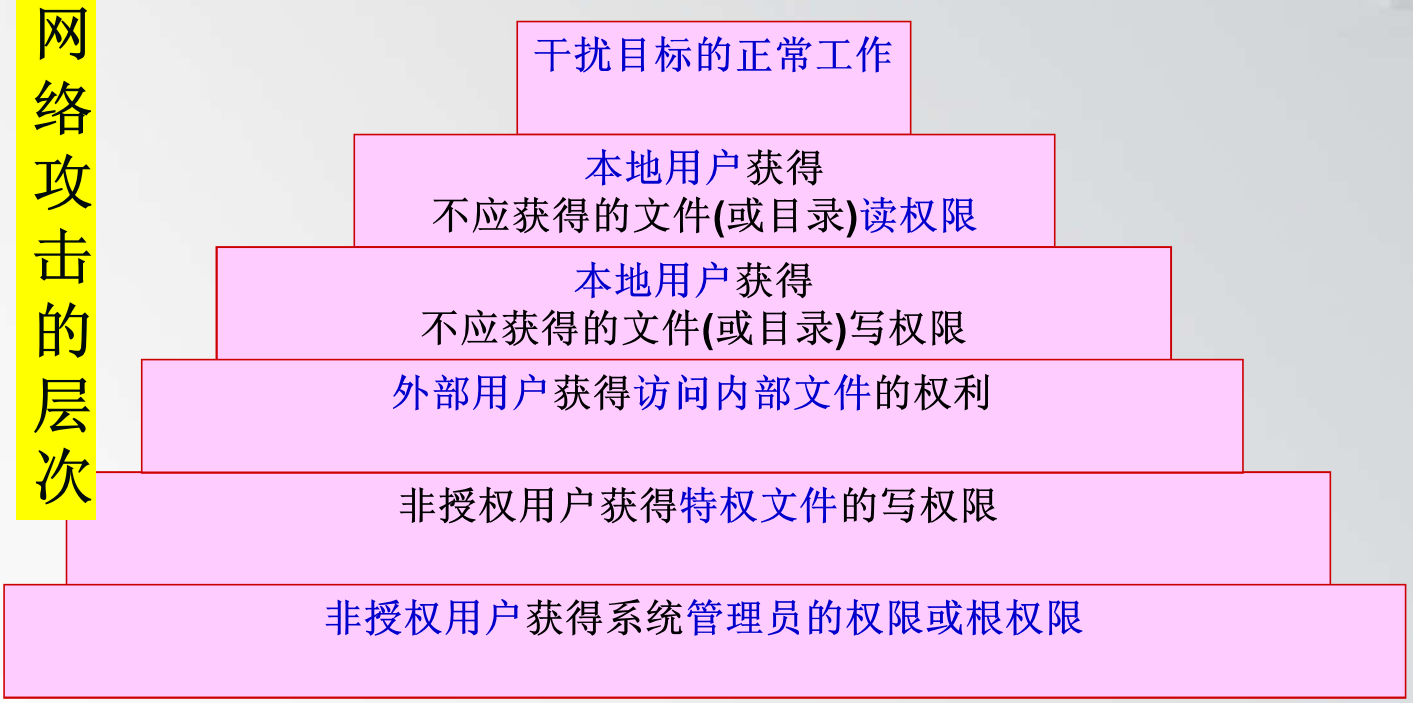
实施安全威胁的人员

- 心存不满的员工
- 软硬件测试人员
- 技术爱好者
- 好奇的年青人
- 黑客（**Hacker**）
- 破坏者（**Cracker**）
- 以政治或经济利益为目的的间谍

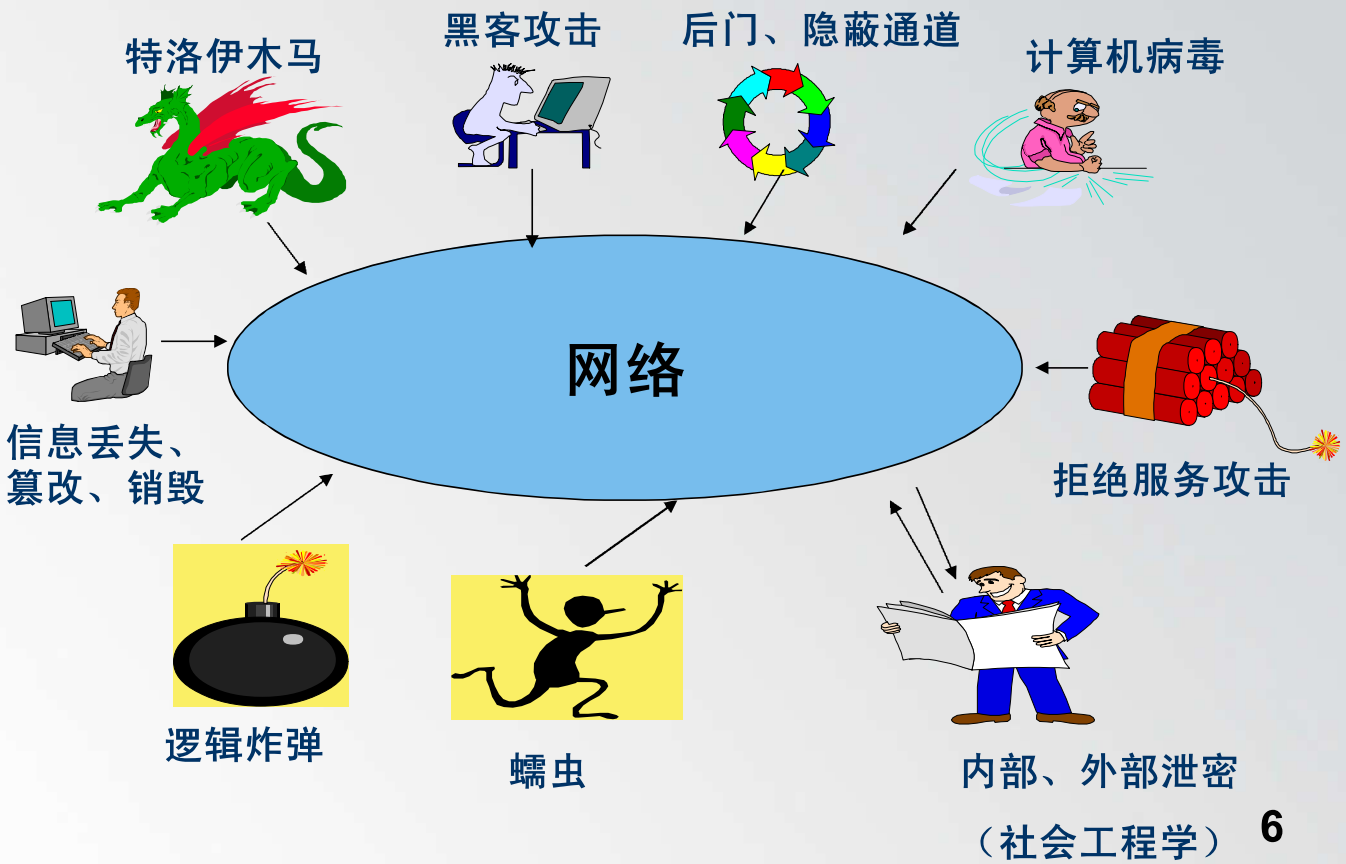
互联网上的黑色产业链


木马制作者
（利益驱使、技术驱使或心理驱使）
病毒批发商
病毒批发商
几乎所有的批发或者零售者都有在木马中留有后门
零售商
零售商
专职盗号者
黑客
肉鸡
肉鸡
肉鸡
肉鸡
QQ被盗
游戏号游币和装备被盗
上行股等操纵
隐私信息被盗
QQ号码、游戏帐号、装备、游戏币、网银等
销赃平台或销赃者

网络攻击的层次


干扰目标的正常工作
本地用户获得
不应获得的文件(或目录)读权限
本地用户获得
不应获得的文件(或目录)写权限
外部用户获得访问内部文件的权利
非授权用户获得特权文件的写权限
非授权用户获得系统管理员的权限或根权限

网络安全目前存在的威胁



安全软肋——社会工程学

社会工程学（**Social Engineering**），是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。

社会工程师，一个无所顾忌的魔术师，用他的左手吸引你的注意，右手窃取你的秘密。他通常十分友善，很会说话，并会让人感到遇上他是件荣幸的事情。

- 凯文·米特尼克Kevin David Mitnick
  - 1964年美国洛杉矶出生，有评论称他为世界上“头号电脑骇客”，他的名字几乎成为黑客的同义词。
  - 技术也许并不是最好的，但是其黑客经历的传奇性足以让全世界为之震惊。美国司法部曾经将米特尼克称为“美国历史上被通缉的头号计算机罪犯”，他的所作所为还被记录在两部好莱坞电影中，分别是《Takedown》和《Freedom Downtime》。
    - 15岁时闯入“北美空中防务指挥系统”的主机，翻遍了美国指向前苏联及其盟国的所有核弹头的数据资料，然后溜之大吉；
    - 24岁时被DEC指控从公司网络上窃取价值100万美元的软件并造成了400万美元损失，被警察当局认为，只要拥有键盘就会对社会构成威胁；
    - 1994年，成功入侵美国摩托罗拉、NOVELL、SUN、MICROSYSTEMS，芬兰的诺基亚等高科技公司的计算机，FBI推算其盗走的程序和数据而造成的实际损害总额达至4亿美元；
    - 他因为入侵计算机专家、黑客Tsutomu Shimomura的计算机而被追踪，落网。在长达5年零8个月的单独监禁之后，2000年米特尼克获得监督释放。但不准触摸计算机、手机以及其他任何可以上网的装置；
    - 美国联邦调查局将他列为头号通缉犯、好莱坞根据他的事迹为蓝本拍摄了电影、以他为主角的书籍更是已经超过10本……
  - 2002年底，凯文·米特尼克完成出版了《欺骗的艺术》一书，立即成为畅销书风靡一时。米特尼克现在的身份是一位计算机安全作家、顾问和演讲者

参考百度百科

- **斯坦利•马克•瑞夫金Stanley Mark Rifkin**
  - 三个电话，一千零二十万美元；
  - **70**年代末，没有雇用帮手、没有使用武器、没有天衣无缝的行动计划，“甚至没有计算机的协助”，依靠一个进入电汇室的机会，然后打了三个电话，成功地将一千零二十万美元转入自己在国外的个人账户。
  - （实际上综合了其他因素：本身了解内部工作机制，工作人员密码暴露等）
  - 这一事件以“史上最大的计算机诈骗案”为名被收录在吉尼斯世界纪录中。

制度的建设、人的管理、 主观的安全防范意识很重要

伊凡的入侵

一个名为伊凡•彼得斯的年轻攻击者把目标锁定在了某公司一款新游戏的源代码上。

【基础】：其朋友利用未修补的Web服务漏洞已攻陷了该公司的一台Web服务器，而这个系统被设置成双定位主机，这意味着他得到了一个内部网络的入口

【进一步入侵】：

①确认服务器类型（社会工程攻击）

- 打到IT技术支持部门，声称自己是公司的员工，他的团队为产品设计了一个界面，然后询问游戏开发团队项目经理的电话号码。
- 伪装成IT部门的人打给开发团队经理。“今天晚上，我们要更换一个路由器，需要确认你的团队里的人是否能连接你们的服务器，所以我们想要知道你的团队用的是哪个服务器。”没有麻烦地回电话验证他所说的事情，或写下他的名字和电话号码，对方直接给出了服务器名称，**ATM5和ATM6。**

伊凡的入侵

大多数系统攻击的第一步都是远程扫描出一个弱口令账户，这是进入系统的最初入口。

②扫描账户（在线）

伊凡知道大多数公司使用的都是基于**Windows**的服务器，他下载了一个名为**NBTEnum**的**NetBIOS**（**BIOS**：基本输入输出系统）列举工具。他输入了**ATM5**服务器的**IP**（**Internet protocol**，**Internet**协议）地址，然后开始运行程序。列举工具能扫描出服务器上存在的账户。

伊凡的入侵

③口令字典攻击（在线）

一旦扫描出存在的账户，可以使用同一个列举工具对计算机系统进行字典攻击（使用常用单词对系统上每个用户的密码进行尝试）。

人们选择的密码，多数都是人名、地名或字典上的常用词。字典攻击可以非常迅速地把常用单词当成密码去尝试一个或多个用户账户。

伊凡第一次尝试了一张包含800个常用词的列表，程序也可以在每个单词的前后添加数字或当前月份。运气不好，没有成功。第二次伊凡下载了一整部电子英语字典，又利用Google搜索 “单词列表 字典”并找到了数千个包含大量单词列表和字典的站点，然后将列表扩充。二十分钟后，它得到了一个账户的密码：“Frodo”——《魔戒》中一个矮人的名字。

伊凡的入侵

- 好消息与坏消息

【好消息】：伊凡破解了**ATM6**服务器的账户拥有管理员权限，他可以登录**ATM6**。

【坏消息】：要找的游戏源代码不在**ATM6**上，而针对**ATM5**的字典攻击没有成功；

- 线索

一个用户可能同时使用**ATM6**和**ATM5**；而用户使用同一个密码的几率很高。下一步可以破解**ATM6**的口令文件，并去**ATM5**上在线尝试各账户。

伊凡的入侵

④口令暴力攻击（离线）

有了“**Frodo**”，伊凡得到**ATM6**的口令文件；通过网络，伊凡拿到一个暴力破解工具**L0phtcrack3**，它会帮助他尝试每一种可能的字母、数字、符号组合对密码进行破解——即使一些系统对口令文件中的密码进行了散列值形式的“加密”。

几个小时后，他得到了**ATM6**上每一个开发小组成员的账户和密码。

⑤通过对**ATM5**在线尝试，他真的找到了某个小组成员，他在**ATM5**和**ATM6**使用的密码都是“**garners**”。

伊凡的入侵

大门向着伊凡敞开了，他自由地搜寻着他想要的程序，直到他找到了源代码的目录并愉快地下载了下来。

然后他进行了系统入侵中典型的一步：他修改了一个隐匿用户（管理员权限）的密码，以防将来想要获得软件的更新版本。

问题出在了哪里

- 严格管理内部入口，及时更新服务器的各种补丁，堵住漏洞；
- 不要轻易相信某个人声称的身份，适当的验证：回拨电话、记录名字等信息；
- 不要用弱口令，不要总用同一份口令；

名词

- 任何以干扰、破坏网络系统为目的的非授权行为都称之为网络攻击。网络攻击实际上是针对安全策略的违规行为、针对授权的滥用行为与针对正常行为特征的异常行为的总和。系统攻击(入侵)：指利用系统安全漏洞，非授权进入他人系统（主机或网络）的行为。
- 黑客（**hacker**）
  - 源于英语动词**hack**，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。一般认为，黑客起源于**50**年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。**60**、**70**年代，“黑客”指代那些独立思考、智力超群，对电脑全身心投入，对计算机的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献的精英。“黑客”通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统;“黑客”能使更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。极富褒义色彩。
  - 现阶段，黑客仍在电脑防护领域充当着重要角色；
- 骇客（**cracker**，**intruder**）
  - 社会的信息化使信息空前繁荣，私有性也越来越强，黑客活动逐渐受到限制；
  - 出现另一种入侵者，利用网络漏洞破坏网络；他们也具备广泛的电脑知识，但与黑客不同的是他们以破坏为目的。

一、黑客攻击的三个阶段

1）收集信息

- 可结合一定的社会工程学手段，利用现有的技术经验和相关基础信息，获取并分析目标的位置、路由、系统结构及技术细节等

- 可利用的工具或协议有：
  ping：测试一主机是否处于活动状态、到达它的时间等；
  Tracert：获取到达某主机经过的网络及路由器列表；
  Finger协议：用于获取某主机上所有用户的详细信息；
  DNS：该服务器提供了系统中可以访问的主机**IP**和机器名列表
  SNMP：可查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构等内部细节；
  whois协议：该协议的服务信息能提供所有关于**DNS**域的相关管理参数

2）探测系统安全弱点

- 根据收集信息，对目标网络上的主机进行探测，以发现系统弱点和安全漏洞；

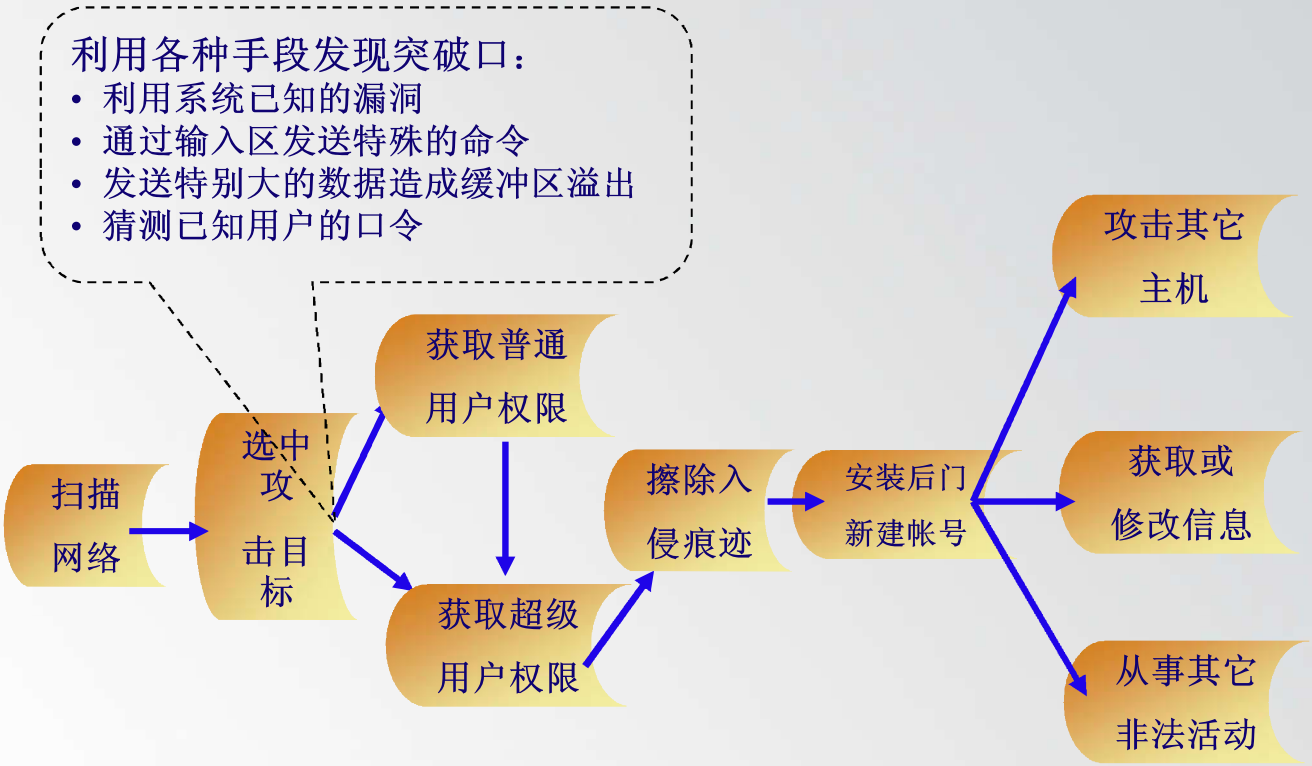
- 主要方法：
  - 利用补丁找突破口：开发商公布的每个“补丁”都明示了系统有哪些需要弥补的漏洞；利用这些“补丁”透漏的信息，可针对未及时修补系统漏洞者实施针对性的攻击；
  - 利用扫描器发现漏洞：扫描器是常用网络分析工具，可对整个网络或子网进行扫描，寻找漏洞。理员管也可利用它发现自身弱点。（**ISS**，**SATAN**等）

3）实施攻击

针对找出的弱点实施攻击

- 掩盖行迹、预留后门
- 安装探测程序：攻击者退出后由探测程序继续监视用户操作，收集感兴趣信息并不断回送给攻击者。
- 取得特权、扩大攻击范围：若能进一步提升信任等级，整个系统将受到全线攻击。

网络入侵步骤总览


利用各种手段发现突破口：
• 利用系统已知的漏洞
• 通过输入区发送特殊的命令
• 发送特别大的数据造成缓冲区溢出
• 猜测已知用户的口令
扫描网络
选中攻击目标
获取普通用户权限
获取超级用户权限
擦除入侵痕迹
安装后门新建帐号
攻击其它主机
获取或修改信息
从事其它非法活动

二、常用攻击技术

1. 破解口令
2. 端 口 扫 描
3. 网 络 监 听
4. IP欺骗、ARP欺骗
5. 拒绝服务攻击
6. 特洛伊木马
7. E-mail 炸 弹
8. 缓冲区溢出

1. 破解口令

口令往往是突破口，攻击者常通过各种方法获得

① 网络监听（一些应用协议如：telnet,ftp,http,smtp等，协议数据包中的帐户和口令是明文传输，容易被获取收集）

② 字典攻击，或穷举攻击口令文件

③ 人为暴露或社会工程骗取

【防范】

- 设置安全的口令：口令的选择字母数字及标点的组合。易记与安全的矛盾。如可使用一句话的开头字母做口令，如：由A fox jumps over a lazy dog!产生口令：AfJoAld!。
- 注意保存：记住、放到安全的地方，最好加密，不能暴露。
- 谨慎使用：隐蔽输入；不要习惯使用同一口令；定期改变口令。

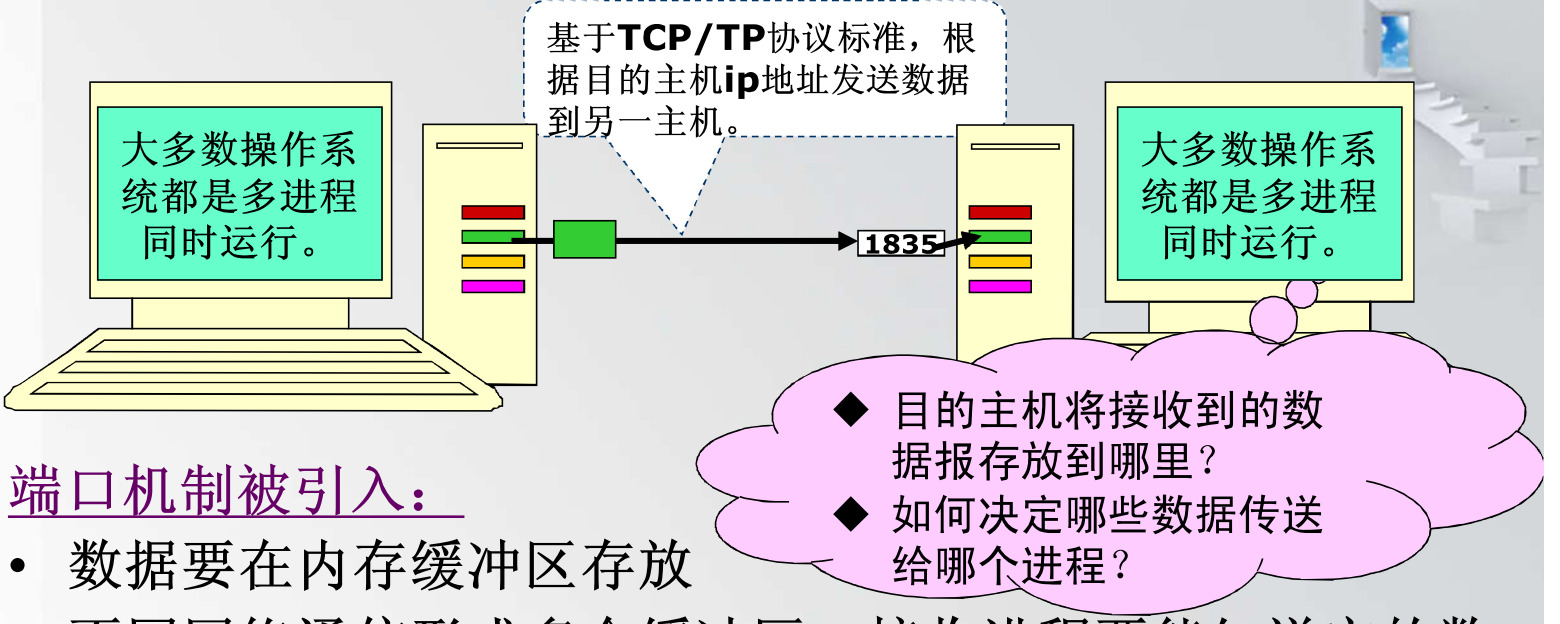
2. 端 口 扫 描

【什么是端口port】

计算机与外界通讯交流的出口。

硬件领域的端口又称接口，如：USB端口、串行端口等。

软件领域的端口：是一种抽象的软件结构，包括一些数据结构和I/O缓冲区。一般指网络中面向连接服务和无连接服务的通信协议端口。



端口机制被引入：

- 数据要在内存缓冲区存放
- 不同网络通信形成多个缓冲区，接收进程要能知道它的数据在哪个缓冲区里。
  - 端口其实就是不同进程的数据缓冲区的编号标志。
  - 操作系统给有网络通信需求的进程分配协议端口（**protocal port**，即我们常说的端口）使进程知道到哪里领取它的数据。
  - 当目的主机接收到数据报后，将根据报文首部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会领取数据并等待下一组数据的到来。

一个端口就是一个潜在的通信通道，也是一个潜在的入侵通道。

- 凡是有网络通信的进程都要被分配一个对应的数据区域，用端口号来标识，到来的数据报按规定的数据格式，被推入目的端口相应的数据区排队，等待被进程取用。
- 不光接受数据报的进程需要开启它自己的端口，发送数据报的进程也需要开启端口，这样，数据报中将会标识有源端口，以便接受方能顺利的回传数据报到这个端口。

【端口分类】

- 端口号由16位二进制数据表示，范围0~65535。分为：

① 公认端口（Well Known Ports，0~1023）紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务的协议。（HTTP-80，FTP-21，TELNET-23，SMTP-25，DNS-53，SNMP-169）

② 注册端口（Registered Ports，1024~49151）松散绑定于一些服务。接收服务请求后从1024开始分配给任务新的端口供通信；

③ 动态和/或私有端口（Dynamic and/or Private Ports，49152~65535）理论上，不应为服务分配这些端口。

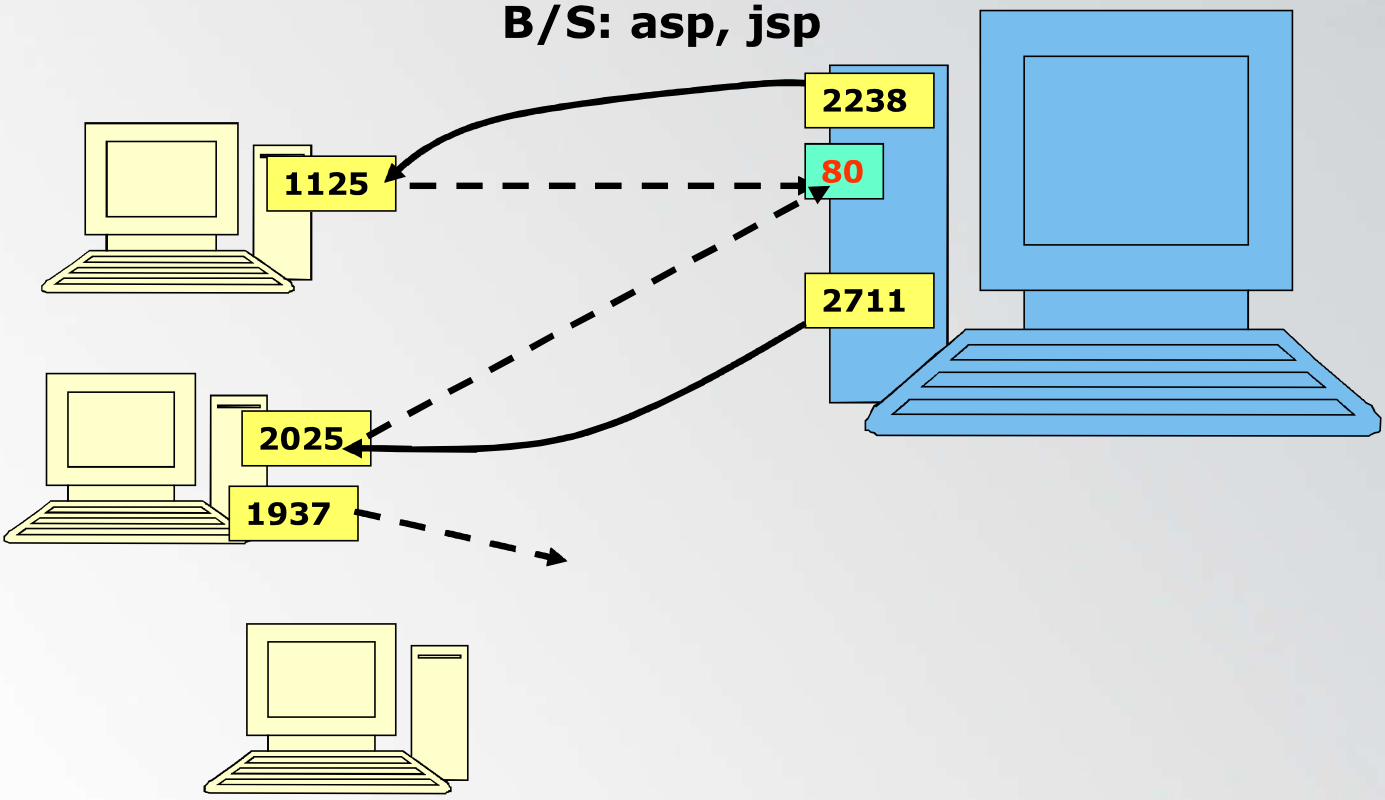
【网络服务使用端口的过程】

在**TCP/IP**网络应用中，通信的两个进程间相互作用的主要模式是客户/服务器模式（**Client/Server model**），操作过程采取客户主动请求服务器被动接收方式。所以，服务进程一般先于客户请求启动。

面向连接的方式为例

服务程序的工作模式：**C/S: vb, vc, java;**

B/S: asp, jsp



网络服务使用端口的过程描述

① 客户端需要通信的进程，随机选择一个端口（在客户机端口上），利用该端口向外发送请求数据包。

② 服务器服务程序运行着一个守护进程（在服务器某固定端口上）如：**WWW**服务的**HTTP**协议在**80**端口上，监听任何发到**80**端口上的服务请求。

③ 当有请求到达时，服务器就启动一个“服务子进程”并与其通信。（在服务器机器上新分配的一端口上）

④ 服务器**80**端口接到一个请求就分配一个新端口如**2530**与该客户通信，将要求的服务信息通过此端口发送回客户。然后继续在**80**口监听。

端口扫描

- 对目标计算机进行端口扫描，能得到许多有用的信息（该机器提供了哪些服务、TCP端口分配了哪些，网络结构如何等）
  - 尝试连接某主机的**23**端口，若是打开的，则说明该机器的**telnet**服务是开启的；
  - 向该机器的**23**端口发送请求信息，根据返回信息搜集相关情报；
- 【手工扫描】要熟悉各种命令。对命令执行后的输出进行分析。
- 【软件扫描】软件都有分析数据的功能。扫描器是检测远程或本地系统安全脆弱性的软件，也可为管理员所用；检测自身是否存在已知漏洞，缩短日常系统安全维护的检测时间。

【扫描器】通过选用远程**TCP/IP**不同端口的服务，记录、分析目标给予的回答，得到关于目标主机的各种有用的信息。

- 好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。
- 编写扫描器程序必须要很多**TCP/IP**程序编写和**C, Perl**和或**SHELL**语言的知识。需要一些**Socket**编程的背景。

- 一般把扫描器分为三类：
  - 数据库安全扫描器
  - 操作系统安全扫描器
  - 网络安全扫描器

分别针对应用程序、网络服务、网络设备、网络协议等。

- 扫描器的使用会产生大量数据传送，加重服务器负担，甚至带有某种风险，所以一般不要轻易使用扫描工具进行频繁扫描。

  常见工具：网络安全扫描器**NSS**，安全管理员的网络分析工具**SSTAM**，**ISS**，**Nessus**，**Jakal**，**Stobe**，**IdentTCPscan**等。

典型的端口扫描

① TCP connect( )扫描
② TCP SYN扫描
③ TCP FIN扫描

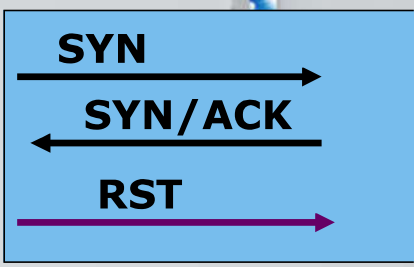
①TCP connect() 扫描
——最基本的TCP扫描方法

- 利用**connect()**系统调用，可与任何感兴趣的目标机器端口进行连接；数据包自动实现三次握手建立连接。
- 若扫描主机响应连接请求，并成功建立连接。说明尝试连接的端口是开放的。否则可判断该端口未开放。

【优点】：任何用户都可执行该调用，可同时打开多个套接字加速扫描。

【缺点】：会被操作系统或工具记录、察觉到端口扫描行为。

②TCP SYN扫描（半连接扫描）



- 尝试连接，但故意使连接不成功建立，被扫描主机察觉不到端口扫描的行为。
  - 攻击者向目标主机发送设置了连接请求（**SYN**）标志的 **TCP** 包，就象打开常规 **TCP** 连接时一样等待反应。
  - 若端口未打开，被扫描主机会返回设置了**RST** 和 **ACK** 标志的包。若端口打开，被扫描主机会返回**SYN/ACK**包进行响应；
  - 攻击者对收到的**SYN/ACK**，回送设置了**RST**的包，将被扫描主机已部分建立的连接关闭。

【优点】：一般系统日志记录的半连接信息较少，不易被发现。有的防火墙会检测到**SYN**扫描。

【缺点】：需要构造适用于该扫描的**IP**数据包，而构造**SYN**数据包需要有权限的高级用户访问专门的系统调用。

③TCP FIN扫描

- 更秘密的一种扫描。通过构造**FIN**（释放连接请求）数据包探测指定端口，关闭的端口会用适当的**RST**来回复**FIN**数据包。打开的端口会忽略对**FIN**数据包的回复。
- 该方法和系统的实现有一定的关系。有的系统不管端口是否打开，都回复**RST**，则这种扫描就不适用。这种方法在区分**Unix**和**NT**时，是十分有用的。

端口扫描相关技术说明

- 基本技术介绍
  - Socket（套接字）

    socket的英文原义是“孔”或“插座”。作为进程通信机制，取后一种意义。是实现端口通信的基本网络编程技术；最初socket是为支持TCP/IP协议而开发，现在它已被认为是开发非RPC (远程过程调用)Windows网络应用程序的最好途径。

- 一般开发一个Server-Client模型的程序，大致包含以下几个基本步骤，具体实现借助Windows 编程的底层API函数:

1）服务器端绑定特定端口，服务器程序在socket1侦听等待连接请求；（socket, bind, listen）
2）客户端通过其socket向服务器和特定端口提交连接请求；(connect)
3）服务器接受连接，产生一个新的socket2绑定另一端口，由此socket2来处理和客户端的交互，服务器继续在原socket1侦听接受其他客户端连接请求；(accept)
4）连接成功后服务器端和客户端就通过读取和写入各自的socket来进行通讯。 (send, recv)

一般客户端socket不与特定端口绑定，随着连接请求动态分配一个1024以上的。

- 一个简单的扫描程序扫描部分的代码：

```
Int main(int argc,char *argv[])
{   …
   for(int i=port1; i< portj; i++){//在设定的端口范围内扫描
      Struct sockaddr_in target_addr;//Socket规定定义的地址结构体
      target_addr.sin_family = AF_INET;//标识协议类型
      target_addr.sin_port = htons（i）; //指明端口号
      target_addr.sin_addr.s_addr = inet_addr（argv[1]）; //获得IP
      cout<<"正在扫描端口:"<<i<<endl;
      If (connect(testsocket, (struct sockaddr*) &target_addr,
                  sizeof（struct sockaddr）) == SOCKET_ERROR )
          cout<<"端口"<<i<<"关闭!"<<endl;
      else
      {   iopenedport++;
          cout<<"端口"<<i<<"开放\n"<<endl;
      }
…                                  *实际上就是一个connect扫描器*
}
```

其他扫描

- 使用ftp代理服务器来扫描tcp端口

  假定S是扫描机，T是扫描目标，F是一个ftp服务器，这个服务器支持代理选项，能够跟S和T建立连接。扫描步骤如下：

  ① S与F建立一个ftp会话，使用PORT命令声明一个选择的端口（称之为p－T）作为代理传输所需要的被动端口。

  ② 然后S使用一个LIST命令尝试启动一个到p－T的数据传输。

  ③ 如果端口p－T确实在监听，传输就会成功（返回码150和226被发送回给S）。否则S回收到无法打开数据连接的应答。

  ④ S持续使用PORT和LIST命令，直到T上所有的选择端口扫描完毕。

其他扫描

- ICMP echo扫描（不是真正意义的扫描，利用ping命令判断网络上一机器是否开机）
- UDP ICMP端口不能到达扫描 （协议比较简单，没有响应包设置，可通过连接错误判断端口是否关闭。错误消息也有丢失率，速度慢，也需要权限）
- TCP反向ident扫描（ident协议允许看到通过TCP连接的任何进程的拥有者用户名，需要在完整的TCP连接基础上实现）
- 。。。。。。

二、常用攻击技术

1. 破解口令
2. 端 口 扫 描
3. 网 络 监 听
4. IP欺骗、ARP欺骗
5. 拒绝服务攻击
6. 特洛伊木马
7. E-mail 炸 弹
8. 缓冲区溢出

3. 网络监听

网络监听可以监视网络的状态、数据流动情况以及网络上传输的信息，是网络管理员监视和管理网络的一种方法，但网络监听工具也常是黑客们经常使用的工具。

网络监听的最大用处是获得有价值的信息，尤其是用户账户及口令。

不同的数据链路上传输的信息被监听的可能性

数 据 链 路	监听的可能性	说　明
Ethernet	高	**Ethernet**网是一个广播型的网络，**Internet**的大多数包监听事件都是一些运行在一台计算机中的包监听程序的结果，这台计算机和其他计算机，一个网关或者路由器形成一个以太网
FDDI **Token_ring**	高	尽管令牌网内在的并不是一个广播网络，但实际上，带有令牌的那些包在传输过程中，平均也要经过网络上一半的计算机，高的数据传输率可以使监听变得困难
电话线	中等	电话线可以被一些与电话公司协作的人或者—些有机会在物理上访问到线路的人搭线窃听；高速的调制解调器将比低速的调制解调器搭线窃听困难一些，因为高速调制解调器中引入了许多频率
IP通过有线电视	高	许多已经开发出来的、使用有线电视信号发送**IP**数据包的系统都依靠**RF**调制解调器，**RF**调制解调器使用—个**TV**通道用于上行；一个用于下行；在这些线路上传输的信息没有加密，因此，可以被一些能在物理上访问到**TV**电缆的人截听
微波和无线电	高	无线电本来就是一个广播型的传输媒介，任何有一个无线电接收机的人都可以截获那些传输的信息

以太网中监听

- 流行的以太网协议工作方式是：将要发送的数据帧发往物理连接在一起的所有主机。在帧头中包含着应该接收数据包的主机的地址。
- 在默认情况下，网络接口读入到达的数据帧，检查数据帧帧头中的地址字段，如果数据帧中携带的物理地址是自己的，或者物理地址是广播地址，则将数据帧交给本机上层协议软件处理，否则就将该帧丢弃。
- 更改主机工作在监听模式下，则不管数据帧的目的地址是什么，所有的数据帧都将被交给上层协议软件处理。

常用监听工具

常用工具：**NetXray,X-Scan,Sniffer,tcpdump,winpcap**

- 嗅探器（**sniffer**）就是一种网络监听工具。将网络适配卡置为**promiscuous**杂乱模式状态，使网卡接受传输在网络上的每个信息包。 **sniffer**工作在网络环境中的底层，它拦截所有的正在网络上传送的数据，并且通过相应的软件处理，可以实时分析这些数据的内容，进而分析所处的网络状态和整体布局。 **Sniffer**实施的是一种消极的安全攻击，它们极其安静地躲在某个主机上偷听别人的通信，具有极好隐蔽性。

- 网络监听对系统管理员是很重要的，系统管理员通过监听可以诊断出大量的不可见问题，这些问题有些涉及两台或多台计算机之间的异常通讯，有些牵涉到各种协议的漏洞和缺陷。

网络监听的检测

- 【是否存在sniffer？】
  - 网络通讯掉包率反常的高，Ping测试的数据包经常无法顺畅流到目的地。
  - 借助带宽控制器观察能看到带宽有异常。某台机器长时间的占用了较大的带宽，这台机器就有可能在听
  - 利用anti-sniffer检查发现sniffer

网络监听的检测

- 【sniffer在哪？】
  - 本机是否被悄悄安装了sniffer：查看本机进程清单，观察。进程的属主和这些进程占用的处理器时间和内存等。（在Unix中通过ps －aun或ps －augx命令——黑客往往在放置监听程序的同时修改ps命令；windows可利用任务管理器。）本方法有一定效果。
  - 用正确的IP地址和错误的物理地址去PING被怀疑的机器（ARP表有关）。（正常的机器一般不接收错误的物理地址的ping信息的，但监听机器就可能接收，要是它的IP stack不再次反向检查MAC的话就会响应。这种方法依赖于系统的IP stack，对有些系统可能行不通。）
  - 往网上发大量包含着不存在的物理地址的包，正常机器不会做处理，但监听程序将处理这些包，将导致sniffer所在机器性能下降，通过比较该机器前后性能（icmp echo delay）加以判断。

网络监听的防范

- 逻辑或物理上对网络分段；（监听往往发生在网段内，所以划分网段的时候可以注意把属于一个信任范围的机器设在一个网段——基于逻辑信任划分，而不是简单的基于物理连接划分）
- 以交换式集线器代替共享式集线器；（共享才导致了网段内的监听），做路由的主机要注意防止被悄悄防置监听程序。安全的布线要从终端就用交换设备。
- 使用加密技术
- 划分**VLAN**，以太→点对点

二、常用攻击技术

1. 破解口令
2. 端 口 扫 描
3. 网 络 监 听
4. IP欺骗、ARP欺骗
5. 拒绝服务攻击
6. 特洛伊木马
7. E-mail 炸 弹
8. 缓冲区溢出

4. IP欺骗

IP SPOOF

1985,贝尔实验室工程师Robbert Morris 在文章“A Weakness in the 4.2BSD Unix TCP/IP Software”中提出的概念。

C发送的冒充包

MACb	MACa	IPb	IPa	TCP头	取消口令检查（伪造的信息）

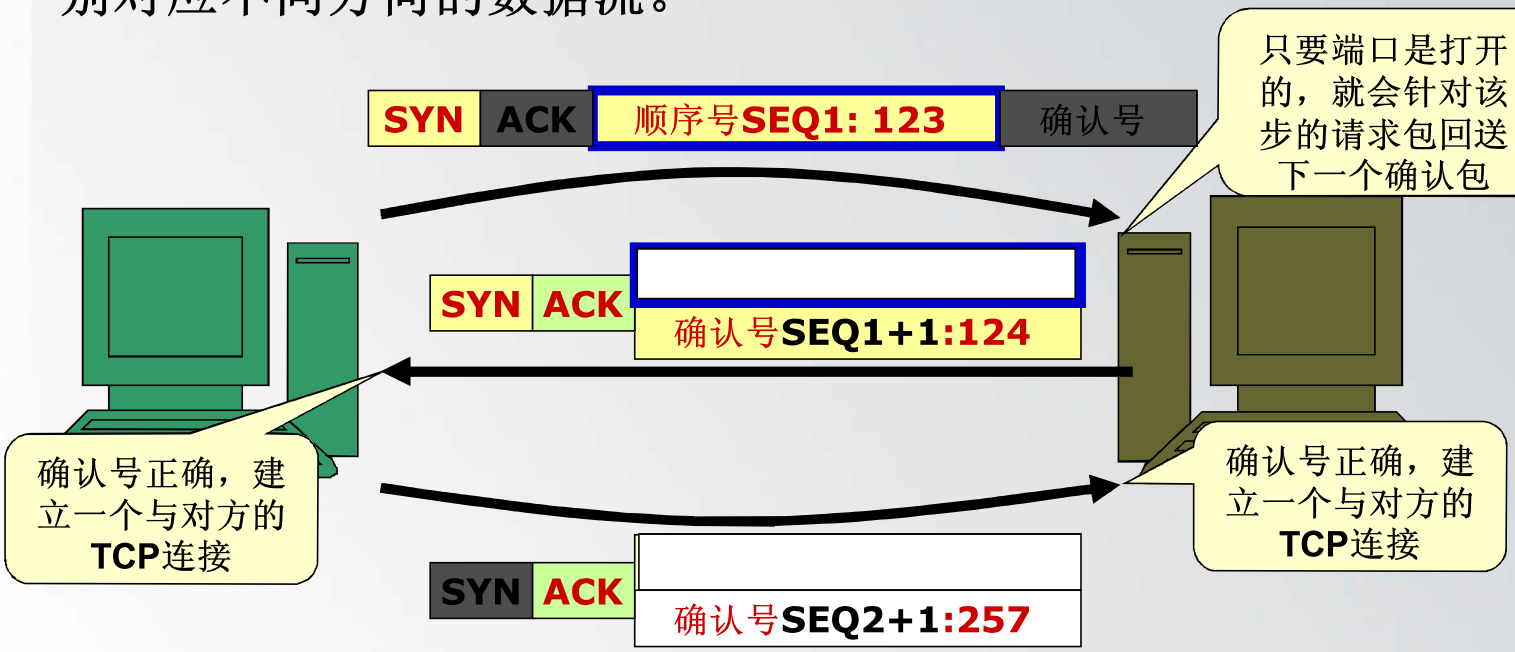
UNIX主机中存在一种特殊的基于地址的信任关系：主机hosta和hostb中已建立两个帐户的相互信任关系。从主机hostb上使用任何以r开头的远程调用命令，如：rlogin、rsh、rcp 等，能无需输入口令验证，直接登录到hosta上。

- 假如能够冒充hostb的IP，就可以使用rlogin类的命令登录到hosta，而不需任何口令验证。

事实上，虽然可以通过编程随意改变发出包的IP地址，但TCP协议对IP进行了进一步封装并控制可靠传输，不会让黑客轻易伪造成功一个合法包。

TCP三次握手过程

- **TCP**连接完全是双向的，即双方的数据流可同时传输。
- 传输中双方数据独立，因此每个**TCP**连接有两个顺序号分别对应不同方向的数据流。



TCP连接成功，双方各自从初始序列号后开始向对方传送数据

握手成功后，开始相互发送数据，
确认号为对方顺序号+接收数据大小

一个单方向传送数据示例

No.	Time (h:m:s:ms)	MAC source addr	MAC dest. addr	Frame	Protocol	A
3	16:8:59:377	00:50:FC:22:C7:BE	00:90:27:F6:54:53	IP	TCP-> FTP	1
4	16:8:59:377	00:90:27:F6:54:53	00:50:FC:22:C7:BE	IP	TCP-> FTP	1
5	16:8:59:377	00:50:FC:22:C7:BE	00:90:27:F6:54:53	IP	TCP-> FTP	1

Addr. IP src	Addr. IP dest	Port src	Port dest	SEQ	ACK	Size
192.168.113.208	192.168.113.1	1064	21	987694419	0	62
192.168.113.1	192.168.113.208	21	1064	1773195208	987694420	62
192.168.113.208	192.168.113.1	1064	21	987694420	1773195209	54

三次握手

No.	Time (h:m:s:ms)	MAC source addr	MAC dest. addr	Frame	Protocol
57	16:9:35:479	00:90:27:F6:54:53	00:50:FC:22:C7:BE	IP	TCP
58	16:9:35:479	00:50:FC:22:C7:BE	00:90:27:F6:54:53	IP	TCP
59	16:9:35:479	00:90:27:F6:54:53	00:50:FC:22:C7:BE	IP	TCP
60	16:9:35:479	00:50:FC:22:C7:BE	00:90:27:F6:54:53	IP	TCP

传数据和回送

Addr. IP src	Addr. IP dest	Port src	Port dest	SEQ	ACK	Size
192.168.113.1	192.168.113.208	1057	1066	1781512762	1052735536	1514
192.168.113.208	192.168.113.1	1066	1057	1052735536	1781514222	54
192.168.113.1	192.168.113.208	1057	1066	1781514222	1052735536	1514
192.168.113.208	192.168.113.1	1066	1057	1052735536	1781515682	54

- **1514**字节=**14**字节以太网头 + **20**字节**IP**头 + **20**字节**TCP**头 + **1460**字节数据
- **58**行显示的应答信号**ACK**为：**1781514222**，这个数是**57**行的**SEQ**序号**1781512762**加上传送的数据**1460**

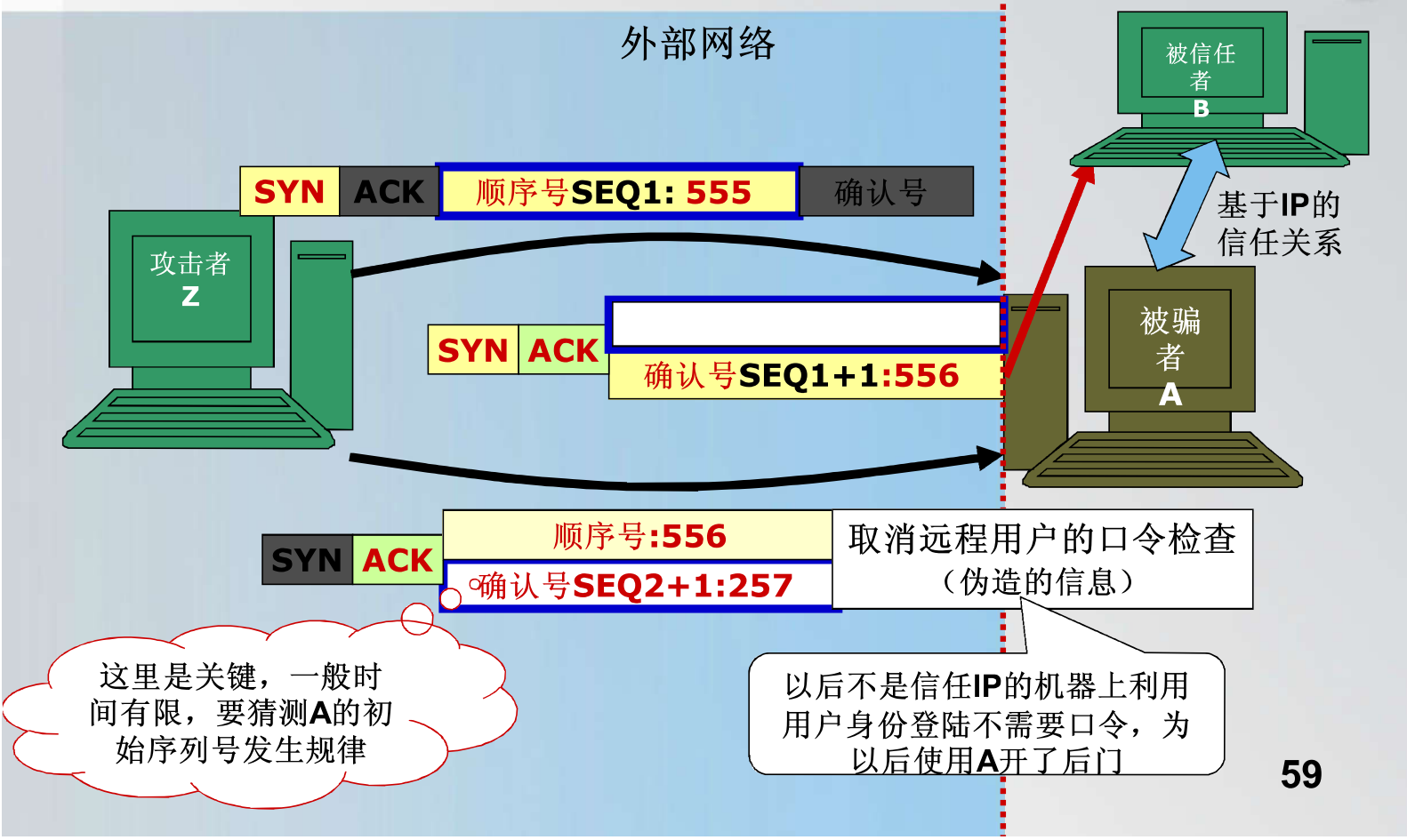
攻击者发送的冒充包

MACb	MACa	IPb	IPa	SYN | ACK	取消口令检查（伪造的信息）

Z要利用伪造IP包攻击对方

- 首先对方得开着端口接收数据；
- 第一次握手请求的**SYN**包一般都会被接收；
- 其他包只有序号正确，才会被对方机器接收。而任意一个**IP**包的序列号都是从初始序列号开始延续下来的。所以，针对一次**TCP**请求，对方的初始序列号是多少很重要。

- 注意Z伪造的包的地址是B的，所以实际上A的回送包都发回给B



IP欺骗的工作原理

- 假设3台主机，A和B相互信任，可通过远程登陆互相访问。Z要冒充B实现与A的连接：

  【准备】选定要攻击的目标A，找出目标主机A的信任模式，并找到一个被信任的B；

  – 使B丧失工作能力，防止冒充时被B揭穿；
  – 采样A的TCP序列号；发起与A的连接，猜测初始序列号，伪造后续数据包，冒充B与A联系。

IP欺骗的工作原理

①使被信任主机丧失工作能力（拒绝服务攻击）

- 使被冒充主机接收不到任何有效的网络数据。如利用TCP机制中处理并行SYN请求有数目上限，使B淹没在大量无意义请求中。

TCP SYN-Flood(攻击三次握手机制)：

【时刻t1】

持续用假IP向B发送大量SYN请求，填满B的TCP队列…

Z（X1）－－－SYN－－－＞B

Z（X2）－－－SYN－－－＞B

Z（Xn）－－－SYN－－－＞B

【时刻t2】

B按照TCP机制向可能不存在的地址回复请求

Xn ＜－－－SYN/ACK--------B

【时刻t3】

X ＜－－－ RST －－－ B

X是不可到达的假主机，所以重复响应若干次后B将回复出错信息

构造的伪造IP包，IP地址和MAC地址都还是B的

Z的主要目的是用正确的序列号让A信任该包中的数据，而这些数据往往是为后面的入侵开路，如传送“echo ++ >>/.rhosts”，从而设置该机器上任何主机都可以无须口令就能访问。

②向A实施欺骗过程

【时刻t1】

Z（B）－－SYN －－－> A

【时刻t2】

B ＜－－－SYN/ACK－－－ A

– A回送的包是发往B的，B已无法接收合法数据，该包将被丢弃，A、B都不会察觉到Z的存在。

【时刻t3】

– Z要和A建立正确的TCP连接并通信，时间有限，只能猜测序列号，构造A的ACK包。

Z（B）－－－ACK－－－＞ A（重点、难点）

【时刻t4】

Z（B）－－－PSH data－－－＞ A

如果上一步猜测成功了，Z就可以用一系列能被A接受的序列号继续构造IP包，持续向A发送数据了。

冒充者实现冒充的关键是正确猜测到要攻击目标A的序列号

序列号取样和猜测的方法举例：

【统计、分析】

- 攻击者可与被攻击主机的一个端口（SMTP是一个很好的选择）建立起正常的连接（以自己的地址）。这个过程重复若干次，并将目标主机最后所发送的ISN（初始序列号）存储起来。
- 攻击者估计其主机与被信任主机A之间的RTT时间（往返时间），这个RTT时间是通过多次统计平均求出的。
  RTT对于估计下一个ISN非常重要。（UNIX序列号发生器一般每秒钟ISN增加128，每次连接增加64。估计ISN的大小，可是128乘以RTT的一半，如果此时目标主机刚刚建立过一个连接，那么再加上一个64。）

【猜测】

- 冒充前先在本机向A产生一个SMTP连接（自己的地址）；然后猜测下一个连接将产生的ISN’；
- 接着，假冒B发送合法TCP连接请求（B的地址，这次请求A很有可能用ISN`为初始序列号），然后用ISN’构造伪造包给A。

IP欺骗的防范

- 抛弃基于地址的信任策略，改用身份验证
- 进行包过滤，从路由器外部进来的源地址却是本地网段IP的包应该过滤掉；
- 使用加密的方法；
- 随机化初始序列号

预测出攻击目标的序例号非常困难，而且各个系统也不相同，序列号猜测并不是容易做到，该攻击方式使用的不算多。

简单盗用IP地址

在同一子网中，可以很轻易的盗用合法的IP地址，惟一留下马脚的是物理地址有可能被记录下来。

盗用另一网段主机的IP地址一般是不行的。因为一般本网段出口路由器对于源地址不属于本网段的数据包不向外转发。

防止盗用IP地址：绑定IP地址和物理地址。

ARP欺骗

- ARP协议并不只在发送了ARP请求后才接收ARP应答，只要计算机接收到ARP应答数据包就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。
- 因此，向局域网中的某台机器发送一个伪造的ARP应答，就可让IP地址指向伪造的MAC；
  - B发送伪造ARP应答包给A：C的IP | B的MAC 。
  - A接收该ARP应答后就会更新本地的ARP缓存，在A看来C的IP地址没有变，但实际上该IP地址已通过MAC地址指向了B。

- 本机ARP表总会定时变旧。而机器和网关是经常通信的，所以，一般arp －a查看本机总是看到一项，就是网关的IP与MAC的对应信息；
- 如果近期和局域网中的某机器通信过，那么也会看到该IP对应的MAC；

问：如果本机a被一个伪造的ARP应答包攻击修改了某机器b的IP指向一个伪造的错误MAC会怎样？如果本机a被一个伪造的ARP应答包攻击修改了网关c的IP指向一个伪造的错误MAC会怎样？该攻击会一直影响a么？

a与b间会不通；a找不到网关无法上网；ARP表的信息过一段时间就会变旧而被删除，所以影响是一段时间内的，除非ARP攻击一直持续。

ARP欺骗是黑客常用的攻击手段之一

- 断网
  - 【攻击路由器】：通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。

    应对：重启路由器以应对；但以后仍难免被攻击；
  - 【攻击主机】：发送假的网关MAC地址给主机，导致主机网络不通或反复掉线。

    应对：利用arp-d命令清除并重建本机arp表；执行后也仍有可能再次遭受ARP攻击；

- 窃取数据

假设网内有三台主机，分别为主机A、B、C。 B在A、C中间实施欺骗：B向A发送一个自己伪造的ARP应答：C的IP | B的MAC；B同样向C发送一个伪造的ARP应答：A的IP| B的MAC。

这样主机A和C都被主机B欺骗，A和C之间通讯的数据都经过了B。ARP欺骗可和其他应用一起实现更复杂的攻击。

发现ARP欺骗

- 运行抓包软件，捕获所有到达本机的数据包。如果发现有某个IP不断发送ARP Request请求包，那么这台电脑一般是病毒源。
- 断网时是否存在ARP攻击：使用arp-a命令检查不能上网的主机，检查网关的MAC是否是实际的网关MAC地址；
- 是否存在ARP攻击：使用arp-a命令检查多台机器，除了网关IP，若都包含另一个IP，则该IP对应的MAC机器频繁和多个机器联系，一般是病毒源。
- 使用“tracert 外网IP”检查不能上网的主机，设缺省网关为10.8.6.1，而跟踪一个外网地址时第一跳却是10.8.6.186，那么，10.8.6.186一般就是病毒源。

ARP的防范

目前对于ARP攻击防护常用的办法有：

1)绑定IP与mac地址（在主机、在路由器上）

以主机为例：

- 获得路由器的内网的MAC地址
- 编写一个批处理文件AntiArp.bat内容如下： @echo off

  arp －d

  arp －s 网关IP 网关MAC
- 计算机重新启动后需要重新进行绑定，因此可将该批处理文件AntiArp.bat文件拖到“开始|启动”中使其开机就执行。

2)使用ARP防火墙(例如AntiArp) 抵御ARP攻击。

防火墙会检测ARP攻击，并以一定频率向网络广播正确的ARP信息 。

也出现了具有ARP防护功能的路由器。

二、常用攻击技术

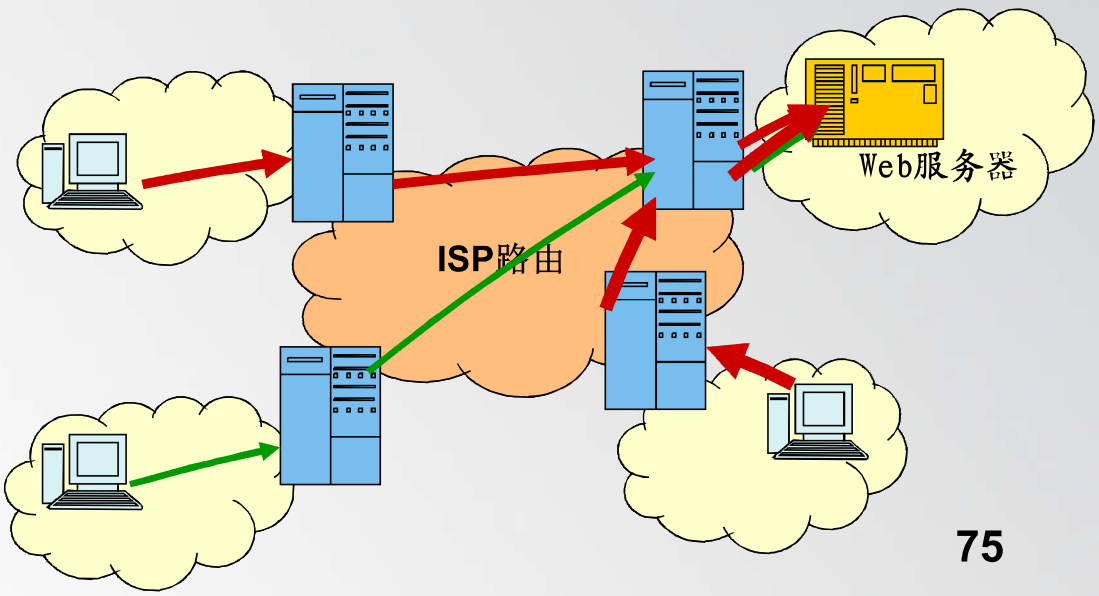
1. 破解口令
2. 端 口 扫 描
3. 网 络 监 听
4. IP欺骗、ARP欺骗
5. 拒绝服务攻击
6. 特洛伊木马
7. E-mail 炸 弹
8. 缓冲区溢出

5.拒绝服务攻击

- 拒绝服务的定义

  拒绝服务（**Denial-of-Service，Dos**）是一种通过耗尽**CPU**、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。

- **Dos攻击对象的资源类型——网络带宽**
  - 网络带宽指连接到ISP的链路容量。通常这个容量低于ISP路由器间的链路容量。
  - Dos攻击下，攻击者直接或间接制造大量流量发往目标服务器，相比合法流量是压倒性的，从而有效拒绝了合法用户对服务器的访问。



- **Dos攻击对象的资源类型——系统资源**
  - 相比消耗带宽更胜一筹，通过过渡加载（利用特殊类型的数据包耗尽服务器上有限的可用系统资源）或使系统网络处理程序崩溃来实现攻击。

①利用数据包耗尽的系统资源可以是：接收数据包的临时缓冲区、打开连接表等类似的内存数据结构。

②利用特殊数据包触发网络处理程序崩溃，从而导致系统崩溃。比如针对早期**windows**操作系统的死亡之**ping**和泪滴攻击，分别针对**ICMP**回送请求包的处理程序和数据包分片处理程序中存在的缺陷。

导致崩溃时，管理员一般要重启目标系统。

- **Dos攻击对象的资源类型——应用资源**
  - 针对特定应用服务程序（如**Web**服务器）的攻击。一般使用一定量的合法请求，而每个请求会消耗大量服务器资源。
  - 如，对提供数据库查询服务的**Web**服务器，构造高代价的、大量的查询请求。这样就限制了服务器响应其他合法用户的查询请求。
  - 或，构造触发服务器程序出错的查询，导致服务器程序崩溃。同样的，除非重启，否则服务器不能响应用户请求。

拒绝服务的目的不在于闯入一个站点或更改其数据，而在于使站点无法服务于合法的请求。入侵者往往并不单纯为了进行拒绝服务而入侵，有时候是为了完成其他的入侵而做准备。

Dos攻击常用的方法

1）源地址欺骗

2）SYN欺骗

3）洪泛攻击

- ICMP洪泛
- UDP洪泛
- TCP SYN洪泛

Dos攻击常用的方法

1）源地址欺骗

- 很多Dos攻击中，使用的数据包采用伪造的源地址，即所谓源地址欺骗。

- 好处
  - 使攻击者隐藏身份。
  - 进一步加大系统的网络拥塞。被攻击目标对发送来的请求包会向源地址回送相应的包，而源地址可能存在、可能不可达，又会反送一些数据包，任何反送的数据包都会加大目标系统的网络拥塞。

一般网络数据包都是在网络通信时通过网络处理程序自动生成并发送出去的。

- 攻击者的特殊数据包怎么制作？

  只要拥有访问某计算机系统上网络处理程序的充分权限（一般需要管理员权限），攻击者就能够制造出需要的包。

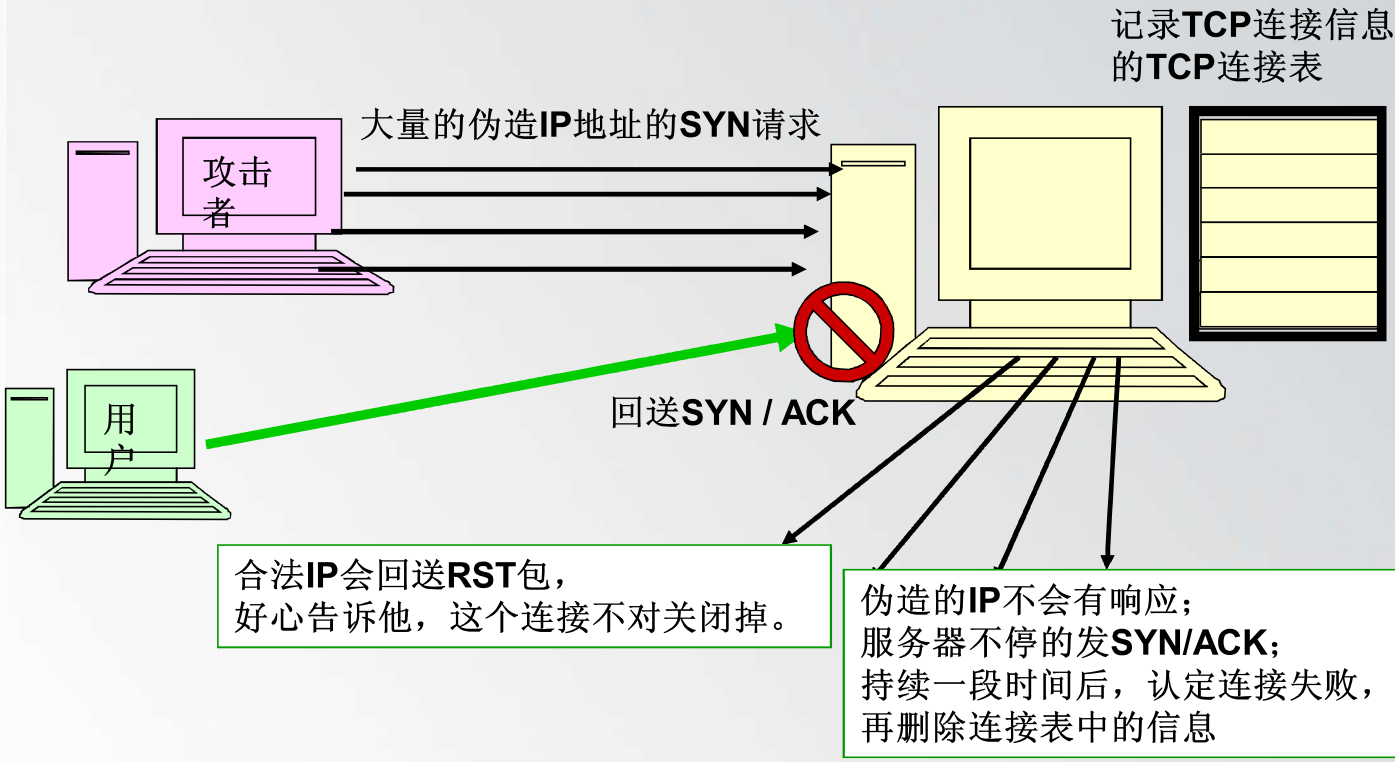
  – 通过操作系统上的原始套接字接口就可以轻松制造数据包（原始套接字接口是操作系统设计者为了网络测试和协议研究而引入的并不是用于正常网络操作用的接口。）
  – 没有上述接口的话就不得不安装一些自定义的设备驱动程序来获得硬件级的设备访问权限。

- 攻击者在哪里？
  - 在攻击者所在机器，利用他的特殊程序生成大量随机源地址，构造数据包实施攻击。
  - 也可能在你的机器上，悄悄安装上他已做好的处理程序，利用你的网卡生成特殊包向被攻击目标发动攻击（往往需要有访问硬件级设备的权限）。
- 对源地址欺骗的包的检查过滤，需要管理路由器的工程师相互合作。过滤应尽可能地接近源系统的路由器上，这样合法源地址的信息越准确。（过滤器最好安装在ISP提供连接的边界上）。

Dos攻击常用的方法

2）SYN欺骗

- SYN欺骗攻击通过造成服务器上用于管理TCP连接的连接表溢出，从而攻击网络服务器相应TCP连接请求的能力。是一种针对系统资源的Dos攻击，具体说就是针对操作系统上的网络处理程序的攻击。


记录TCP连接信息
的TCP连接表
大量的伪造IP地址的SYN请求
攻击者
用户
回送SYN / ACK
合法IP会回送RST包，
好心告诉他，这个连接不对关闭掉。
伪造的IP不会有响应；
服务器不停的发SYN/ACK；
持续一段时间后，认定连接失败，
再删除连接表中的信息

- 关于伪造的源地址
  - **Internet**是有很多未被使用的地址，大范围的随机产生源地址，有相当一部分不会有对应的真实主机。
- 关于网络流量
  - **SYN**欺骗攻击和洪泛攻击在流量上有明显差别。前者只要使**TCP**连接表被填满就行，形成的流量相对比较小，更不会接近与服务器相连的链路的最大容量。
  - 中型的机构甚至宽带家庭用户都可以利用**SYN**欺骗成功攻击大型公司服务器。

- **SYN欺骗变形——land攻击：**

  一个特别打造的**SYN**包中的源地址和目标地址都被设置成某一个服务器地址，这时将导致接受服务器向它自己的地址发送**SYN**一**ACK**消息，结果这个地址又发回**ACK**消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。

  Land攻击通常使存在漏洞的机器崩溃。许多**UNIX**实现将崩溃，而 **Windows NT** 会变的极其缓慢。

【 防御】打最新的补丁，对防火墙进行配置，将在外部接口上入站的含有源地址是内部地址的数据包过滤掉。

Dos攻击常用的方法

3）洪泛攻击flooding attack

以占据所有到目标机构的网络连接容量为目标，使服务器的链路超负荷的攻击都是洪泛攻击。

几乎任何类型的网络数据包都可以用来进行洪泛攻击，只要数据包能够被运行流到目标系统的链路。数据包越大，攻击效果越好。

根据使用的网络协议不同，洪泛攻击可以划分为不同类型，典型的有：

①**ICMP**洪泛

②**UDP**洪泛

③**TCP SYN**洪泛

①ICMP洪泛

- ICMP协议是一种面向无连接的协议，用于传输出错报告控制信息。从技术角度来说就是一个“错误侦测与回报机制”，在检测网路的连线状况方面ICMP 是个非常有用的协议。
- 回送请求数据包的ping flooding是典型的ICMP洪泛。
- 向目标主机长时间、连续、大量地发送ICMP类型数据包，也会最终使系统瘫痪。

【防范】

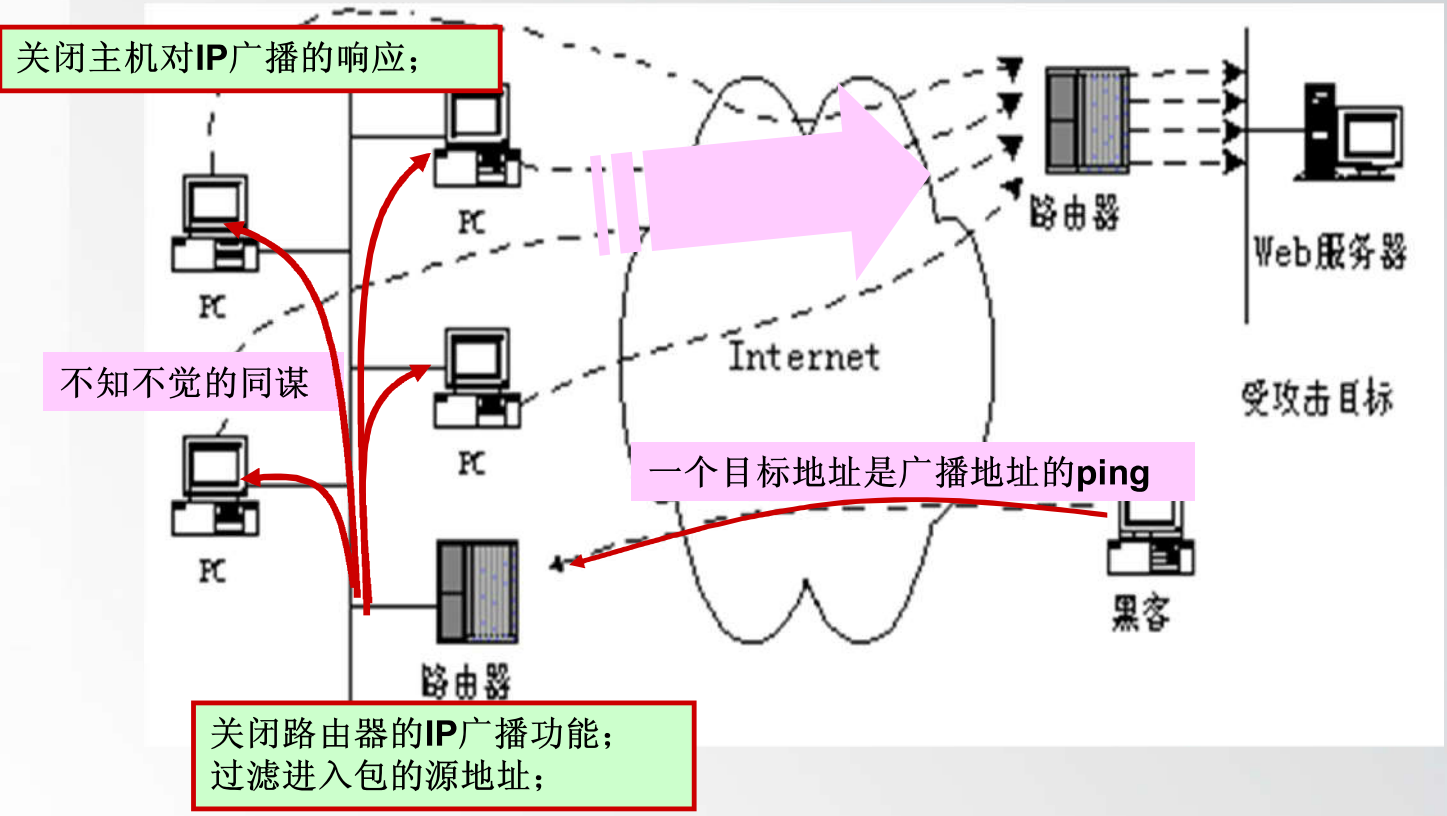
- 第一种方法是在路由器上对ICMP数据包进行带宽限制，将ICMP占用的带宽控制在一定的范围内，即使有ICMP攻击，它所占用的带宽也是非常有限的。
- 第二种方法就是在主机和防火墙上设置ICMP数据包的处理规则。
  - 有时候不能完全阻止ICMP包，如ICMP目的不可达和超时数据包往往作为关键数据包类型需要允许通过。
  - 如：防火墙应该执行一个缺省的拒绝策略：除了出站的ICMP Echo Request、出站的ICMP Source Quench、进站的TTL Exceeded和进站的ICMP Destination Unreachable之外，所有的ICMP消息类型都应该被阻止。

- **Smurf**攻击

这种攻击结合了**IP**欺骗和**ICMP**，以最初发动这种攻击的程序名“**Smurf**”来命名。

伪造的**IP**地址 | 广播地址

发送广播的**ICMP**应答请求**(ping)**数据包，回复地址设置成受害者地址。最终导致网络的所有主机都向被攻击者回送应答请求，导致网络阻塞。


关闭主机对IP广播的响应；
PC
PC
PC
PC
不知不觉的同谋
Internet
路由器
Web服务器
受攻击目标
一个目标地址是广播地址的ping
黑客
路由器
关闭路由器的IP广播功能；
过滤进入包的源地址；

Smurf攻击示意图

②UDP洪泛

攻击者发送UDP包到目标系统提供服务的端口上。UDP数据包常发给诊断回送服务。

- 该服务开启的话，会回应一个带有初始数据内容的UDP数据包给源地址。
- 该服务没开启的话，可能会回应ICMP目的主机不可达的包给源地址。

不管服务是否开启，攻击者都达到了消耗服务器链接容量的目的。

③TCP SYN洪泛

发送大量带有真实或虚假源地址的TCP数据包给目标系统。

TCP SYN洪泛攻击可以是SYN包，也可以是不属于任何已知连接的SYN/ACK包；后一种包，即使连接不建立，攻击者也消耗了被攻击服务器的网络链路。

【两种简单防御办法】

- 第一种是缩短**SYN Timeout**时间，由于**SYN Flood**攻击的效果一部分取决于服务器上保持的**SYN**半连接数，这个值**=SYN**攻击的频度 **x SYN Timeout**，所以通过缩短从接收到**SYN**报文到确定这个报文无效并丢弃改连接的时间，例如设置为**20**秒以下（过低的**SYN Timeout**设置可能会影响客户的正常访问），可以成倍的降低服务器的负荷。

  仅在对方攻击速度和频度不高的情况下生效

- 第二种方法是设置**SYN Cookie**，就是给每一个请求连接的**IP**地址分配一个**Cookie**，如果短时间内连续受到某个**IP**的重复**SYN**报文，就认定是受到了攻击，以后从这个**IP**地址来的包会被丢弃。

  依赖于对方使用真实的**IP**地址

多主机协同的Dos攻击

单一主机的Dos容易被追踪，且受攻击系统上能产生的网络流量总量的限制。复杂的多攻击系统便衍生且被广泛使用，通过多主机协同Dos来进行攻击。

1）分布式拒绝服务攻击

2）反射攻击和放大攻击

1）分布式拒绝服务DDoS(Distributed Denial of Service)

是一种基于DoS的特殊形式的拒绝服务攻击，发起入侵的源是多个，是一种分布、协作的大规模攻击方式。

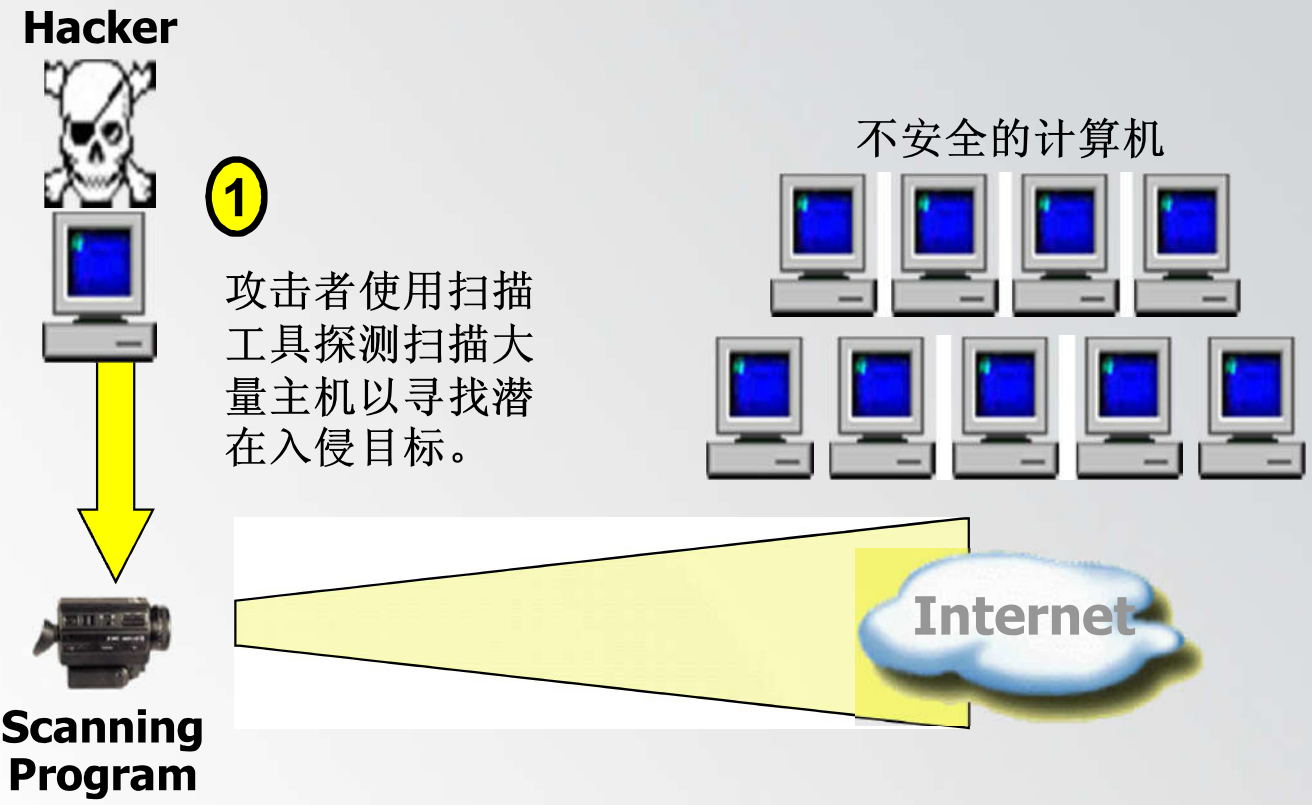
比较完善的DDoS攻击体系分成三层。

- **攻击者：**攻击者所用的计算机，是攻击主控台，可以是网络上的任何一台主机，甚至可以是一个活动的便携机。攻击者由此操纵整个攻击过程，向主控端发送攻击命令。
- **主控端（执行僵尸机）：**攻击者非法侵入并控制的一些主机，安装特定程序分别控制大量的代理主机。接受攻击者发来的特殊指令，并且把这些命令发送到代理主机上。
- **代理端（代理僵尸机）：**同样是攻击者侵入并控制的一批主机，它们上面运行攻击器程序，接受和运行主控端发来的命令。代理端主机是攻击的执行者，由它向受害者主机实际发起攻击。

美国几个著名的商业网站（例如**Yahoo**、**eBay**、**CNN**、**Amazon**、**buy.com**等）遭受黑客大规模的攻击，造成这些高性能的商业网站长达数小时的瘫痪。而据统计在这整个行动中美国经济共损失了十多亿美元。

这种大规模的、有组织、有系统的攻击方式受到各国政府和学术界的高度重视。

分布式拒绝服务攻击步骤1



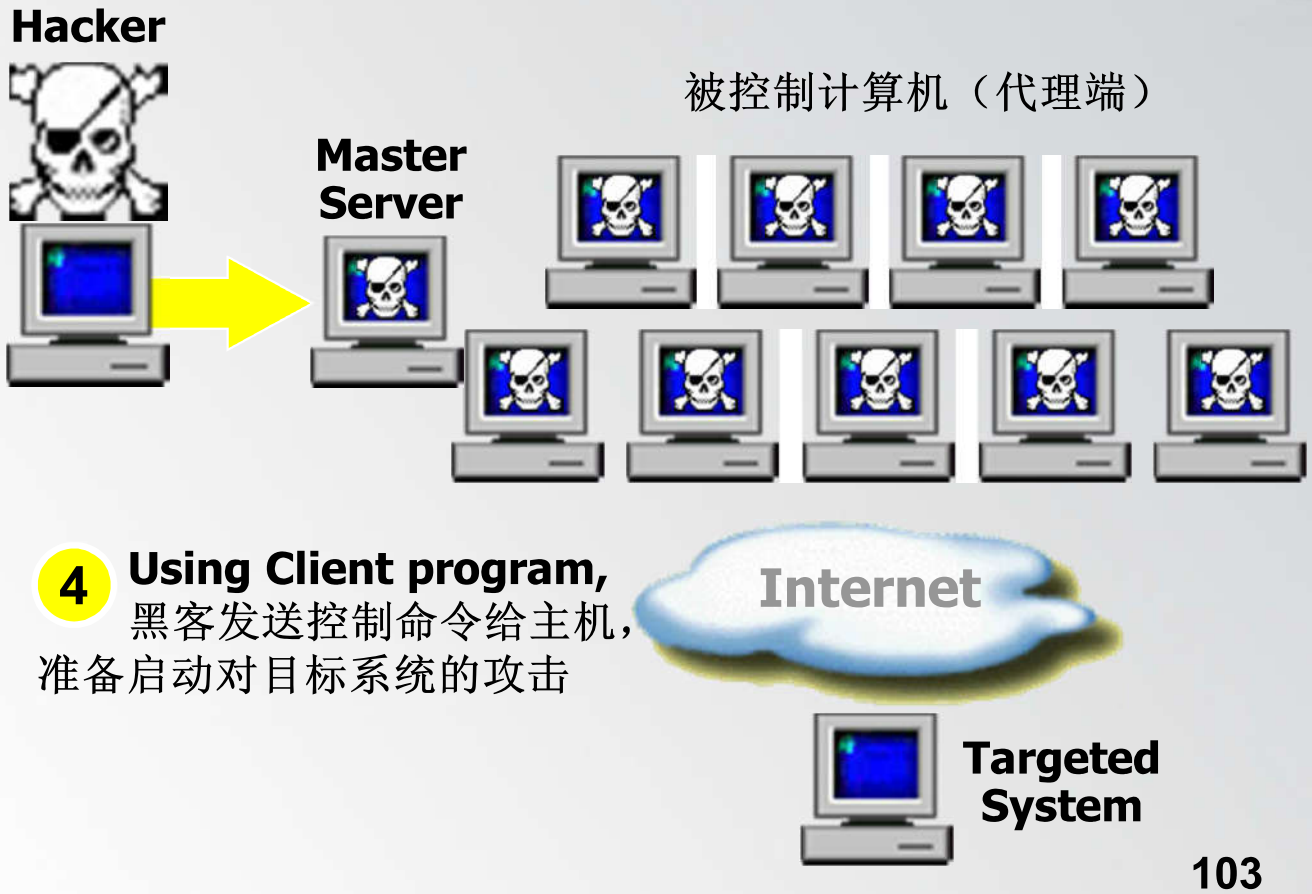
分布式拒绝服务攻击步骤2

黑客设法入侵有安全漏洞的主机并获取控制权。这些主机将被用于放置后门、sniffer或守护程序甚至是客户程序。

分布式拒绝服务攻击步骤3

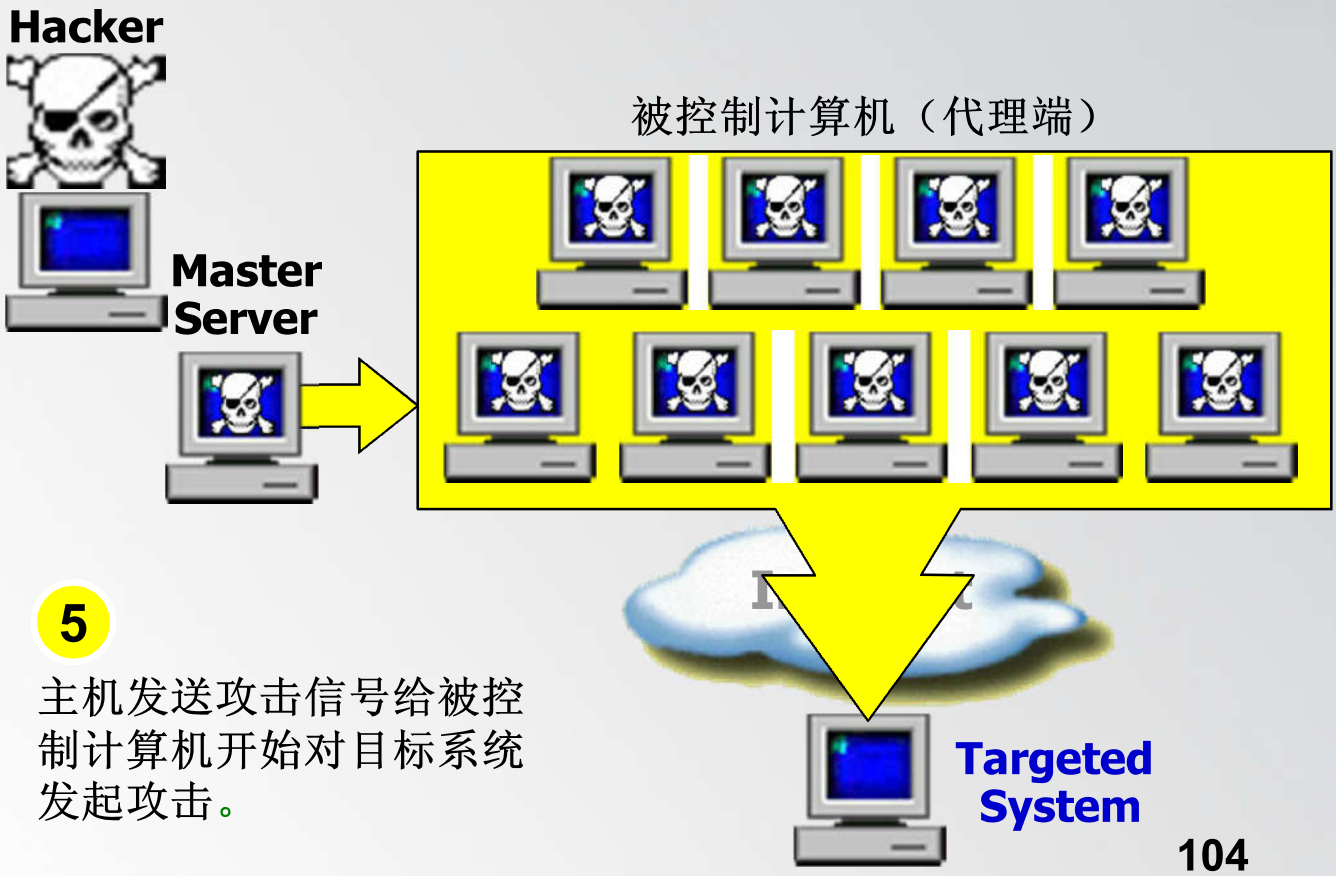
3 黑客在得到入侵计算机清单后，从中选出满足建立网络所需要的主机，放置已编译好的守护程序，并对被控制的计算机发送命令。

分布式拒绝服务攻击步骤4



4 **Using Client program,**
黑客发送控制命令给主机，准备启动对目标系统的攻击

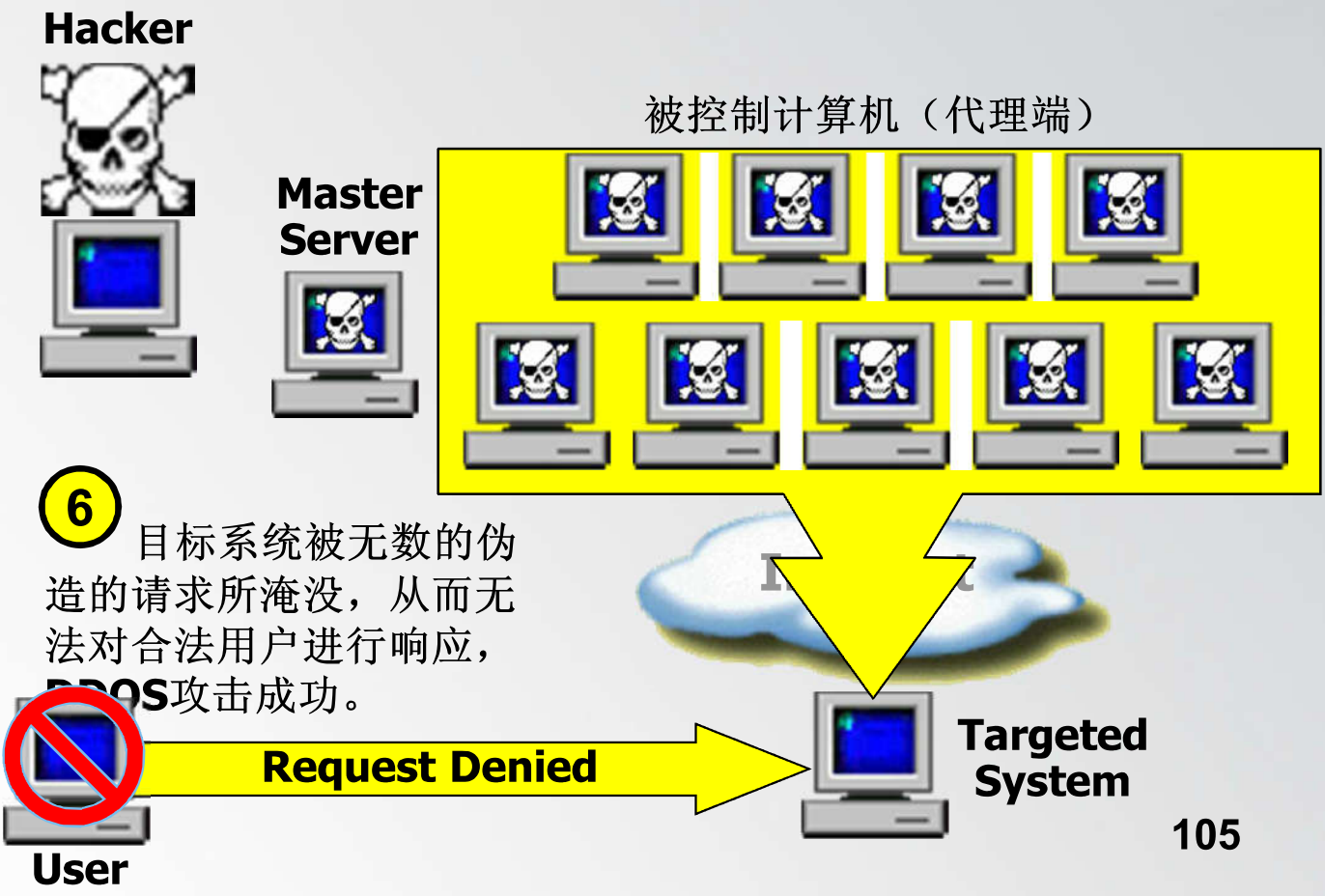
分布式拒绝服务攻击步骤5



5

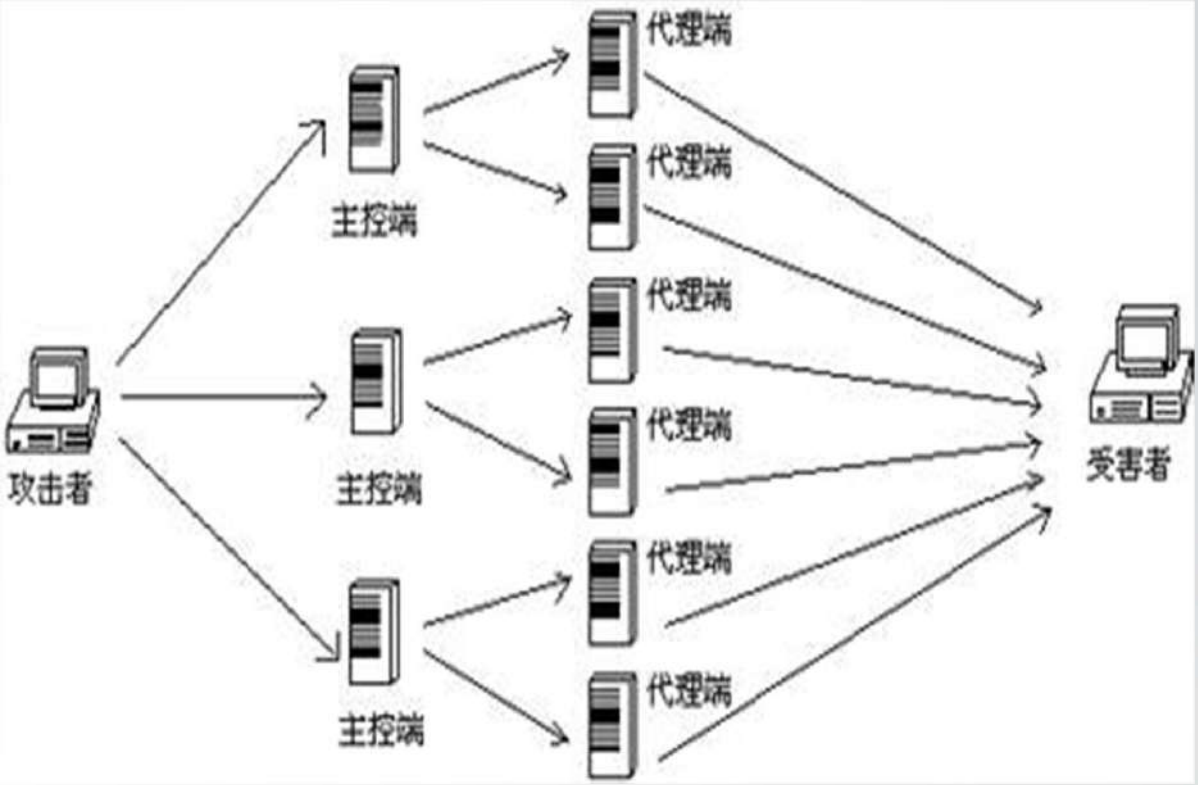
主机发送攻击信号给被控制计算机开始对目标系统发起攻击。

分布式拒绝服务攻击步骤6



由于整个过程是自动化的，攻击者能够在5秒钟内入侵一台主机并安装攻击工具。也就是说，在短短的一小时内可以入侵数千台主机。并使某一台主机可能要遭受1000MB/S数据量的猛烈攻击，这一数据量相当于1.04亿人同时拨打某公司的一部电话号码。

DDOS攻击示意图



为什么使用多层的分布攻击

- 若直接操纵大量代理端发起实际攻击，清理痕迹工作庞大，容易出纰漏而被追查到；

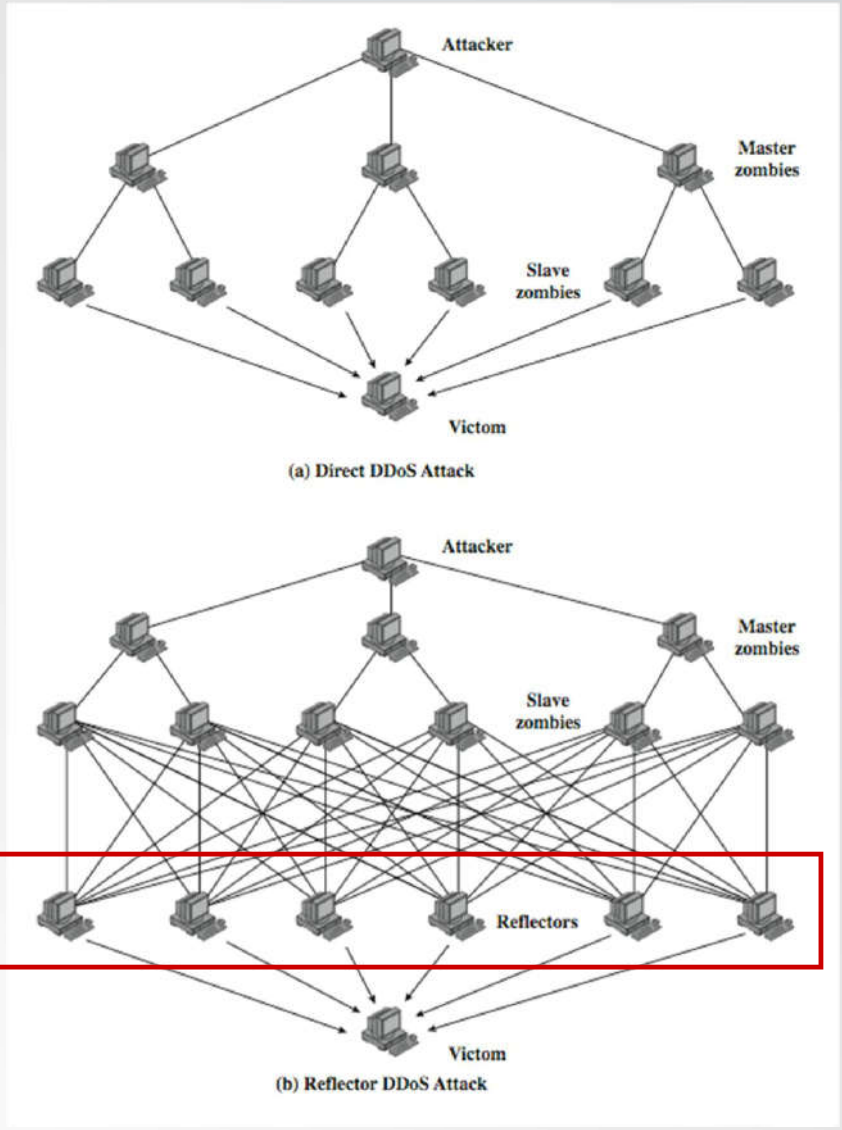
- 使用少数控制端分层，即使通过代理找到控制端，由于控制端数量较少，其清理工作可以做的比较好，很难从其向上追查到攻击者。

2）反射攻击与放大攻击(simple reflection attack/amplification attack)

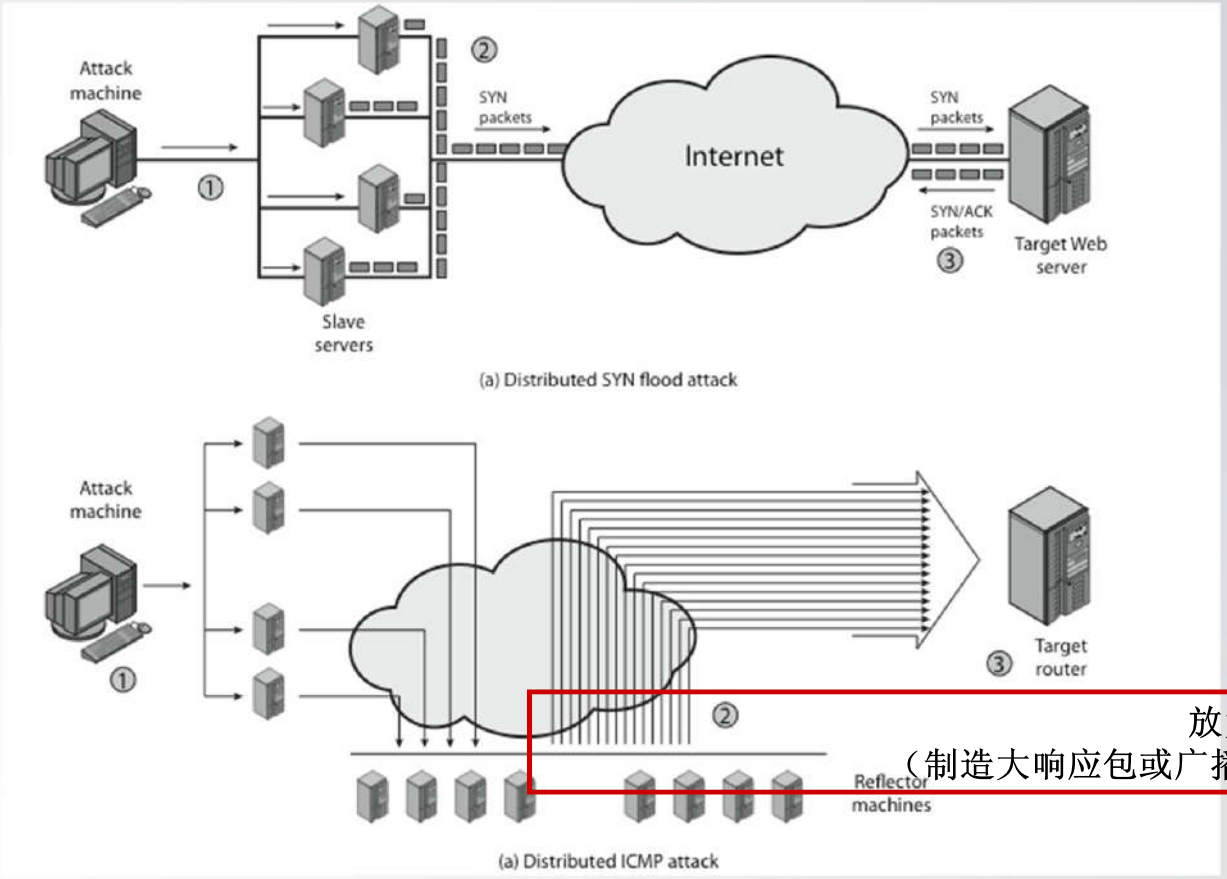
这类攻击的中间媒介除了被控制的僵尸，还利用了很多网络服务系统的正常功能。

通过僵尸发送虚假地址信息，利用正常的网络服务将响应数据包发射或放大回送到被攻击目标。

DDoS Flood Types



反射



放大
（制造大响应包或广播）

分布式拒绝服务DDoS防范

- 攻击预防和先占
  - 调整资源消耗策略、提供后备资源、改善相关协议等。
  - 如提供显著过剩的网络带宽、内容相同的分布式服务器（在超负荷可预料时，如世界杯足球实况直播等）；如改进TCP版本，使用cookie控制连接。如限制网络连接最大速率。如屏蔽IP定向广播的使用等。
- 攻击检测和过滤
  - 有一套识别异常流量的机制，根据数据包的捕获、分析，发现Dos攻击时能判断攻击类型；合理配置过滤器过滤掉攻击数据包。在无法抵御大量的Ddos攻击时能快速切换到备份服务器。
- 攻击源回溯和鉴定
  - 尝试鉴定攻击源也是阻止将来的攻击的先期预防。

二、常用攻击技术

1. 破解口令
2. 端 口 扫 描
3. 网 络 监 听
4. IP欺骗、ARP欺骗
5. 拒绝服务攻击
6. 特洛伊木马
7. E-mail 炸 弹
8. 缓冲区溢出

6.特洛伊木马和病毒

特洛伊木马程序指任何提供了隐藏的、用户不希望的功能的程序。

特洛伊木马程序并不是病毒

- 木马不具有病毒的可传染性、自我复制能力等特性
- 但是特洛伊木马程序具有很大的破坏力，和病毒结合起来更具危害性。

- 木马特点：
  - 隐蔽性：木马的设计者为了防止木马被发现，会采用多种手段隐藏木马；
  - 非授权性：指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表、控制鼠标、键盘等，而这些权力并不是服务端所在机器赋予的，而是通过木马程序窃取的。

特洛伊木马常见类型

①密码发送型特洛伊木马

②键盘记录型特洛伊木马

③远程访问型特洛伊木马

④FTP型特洛伊木马

⑤毁坏型特洛伊木马

①密码发送木马

- 该类木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感密码文件，利用免费的电子邮件服务将搜集的密码等信息发送到指定的邮箱。

②键盘记录木马

- 这种特洛伊木马非常简单，只做一件事情，就是记录受害者的键盘敲击并且在LOG文件里查找密码。这种特洛伊木马常随indows的启动而启动，记录键盘的按键情况，从这些按键中很容易得到密码、账号等信息。对于这种类型的木马，邮件发送功能也是必不可少的。

③远程访问型特洛伊木马

- 数量最多，危害最大的一种木马，以远程控制为目的，也往往集成其他种类木马的功能（键盘记录，上传和下载，注册表操作，限制系统功能等），从而在被感染的机器上为所欲为，可任意访问文件，得到机主的私人信息（甚至包括信用卡，银行账号等）。

④破坏性质的木马

- 该类木马就是破坏被感染计算机的文件系统，使系统崩溃或者重要数据丢失。在这点上和病毒很相像，但这种木马的激活是由攻击者控制的，并且传播能力比病毒逊色很多。

⑤FTP型特洛伊木马

- 该类木马打开用户机器的21端口，使攻击者可以通过FTP客户端不用密码就连接到用户的机器，并且有完全的上传和下载选项。

木马的远程操作原理

以远程控制为目的的木马一般都有客户端和服务器端两个执行程序：

1）通过某种方式将木马程序（服务器端程序）植入到用户的电脑里面，该程序会悄悄的开启一个端口，等待接收控制者的控制信息。

2）利用客户端程序，攻击者可远程控制被植入木马的机器。（攻击者通过INTERNET在服务端和控制端之间建立一条木马通道，必然需要控制端IP/服务端IP，控制端端口/木马端口）

木马的自动加载

- 木马往往随机器启动悄悄运行；
- 特洛伊木马程序行迹一般会在注册表、**win.ini**或**system.ini**文件中，因为系统启动的时候需要装载这些文件。
  - 在**win.ini**文件中的**[WINDOWS]**下面，“**run=**”和“**load=**”都是可能加载特洛伊木马程序的途径。
  - 在**system.ini**文件中，“**shell=explorer.exe**程序名”，后面跟着的程序名就多是特洛伊木马程序。

木马的防范

在对付特洛伊木马程序方面，综合起来，有以下几种办法和措施。

- （1）提高防范意识，不要随意下载或运行陌生的程序。
- （2）多读**readme.txt**文件。
- （3）养成良好的使用习惯，定期查杀。
- （4）发现木马立即断网。
- （5）熟悉系统，观察敏感目录。
- （6）在删除特洛伊木马之前，最重要的一项工作是备份文件和注册表。

7. 邮件炸弹

- **E-mail**炸弹
  - 也是**Dos**攻击的一种。在短时间内连续寄发大量邮件给同一收件人，使得收件人的信箱容量不堪负荷而无法收发邮件。
- 防范：
  - 尽少散播自己的邮箱地址；
  - 设置规则，进行地址过滤；
  - 使用防护工具；

8. 缓冲区溢出

缓冲区溢出攻击是通过在程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈。有目的的溢出能使程序转而执行其他指令，以达到攻击的目的。

【危险表现】

– 能获得系统的最高控制权，而且还很难被检测。

【根源】

– 往往是由于程序中没有仔细检查用户输入的参数，缺陷属于输入确认错误。

思考与作业

思考：

1. 你自身的相关工作有什么安全问题？你能发现别人的什么漏洞？阅读相关案例。
2. 黑客进行系统攻击的三个阶段是什么？
3. 举出4种以上的网络攻击方法，并简单介绍。
4. 什么是扫描器？简单阐述你对端口扫描攻击的认识。
5. TCP connect扫描与TCP SYN扫描的原理与区别。
6. 系统端口分哪几类，公认端口的使用范围是？以下常用服务使用的端口分别是什么：HTTP、FTP、TELNET。
7. Socket在网络编程中是指运行在网络上的两个程序间双向通讯连接的末端，它提供客户端和服务器端的连接通道。简述每个Socket应用从连接的建立到结束，大致包含的几个基本步骤。
8. 以太网结构的主机对数据包的处理方式是怎样的，举例要实现网络监听可利用的工具，并简单阐述网络监听的探测方法。
9. 简述IP欺骗过程，其实现难度高主要源于什么。
10. 简单说明ARP欺骗的原理及表现。
11. Ddos的反射和放大攻击是什么？画出DDos体系图，并简单说明。
12. 简述Smurf攻击过程。