计算机科学导论

——网络攻防

龚文引　博士

计算机学院

目录

- 网络攻防概述
- 安全攻防案例分析
- 常见网络安全技术

目录

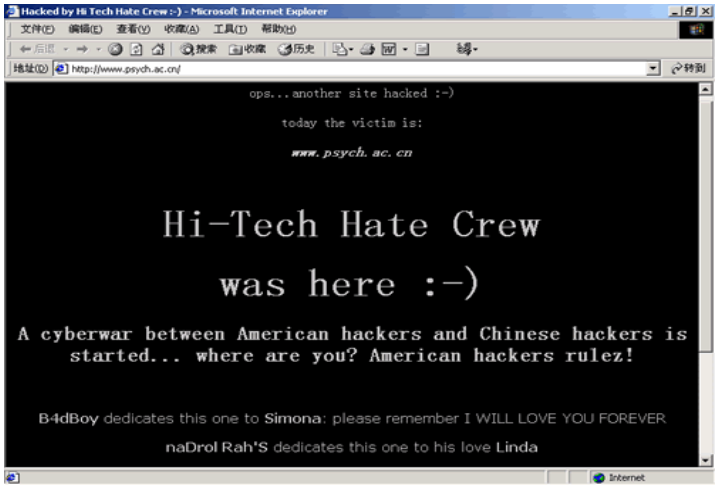
网络攻防概述

- 2001年中美黑客大战
  - 事件背景和经过
    - 中美军机南海4.1撞机事件为导火线
    - 4月初，以PoizonB0x、pr0phet为代表的美国黑客组织对国内站点进行攻击，约300个左右的站点页面被修改
    - 4月下旬，国内红（黑）客组织或个人，开始对美国网站进行小规模的攻击行动，4月26日有人发表了“五一卫国网战”战前声明，宣布将在5月1日至8日，对美国网站进行大规模的攻击行动。
    - 各方都得到第三方支援
    - 各大媒体纷纷报道，评论，中旬结束大战

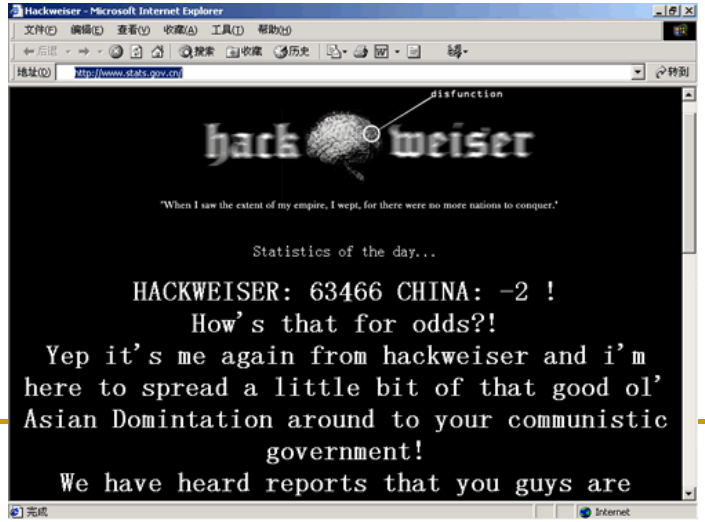
网络攻防概述

国内某大型商业网站

国内某政府网站



中国科学院心理研究所

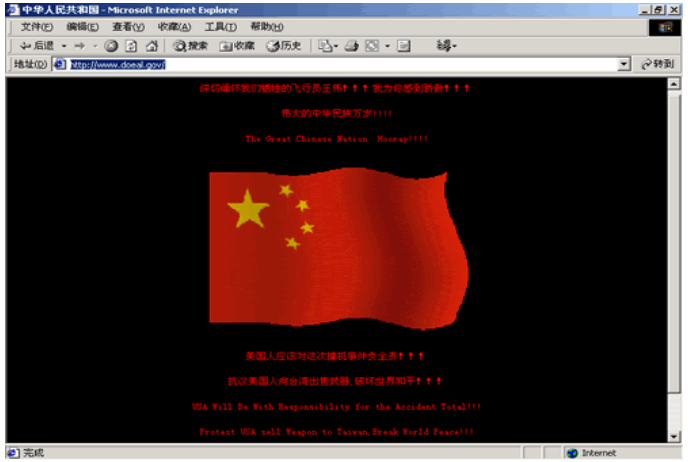


中经网数据有限公司

网络攻防概述

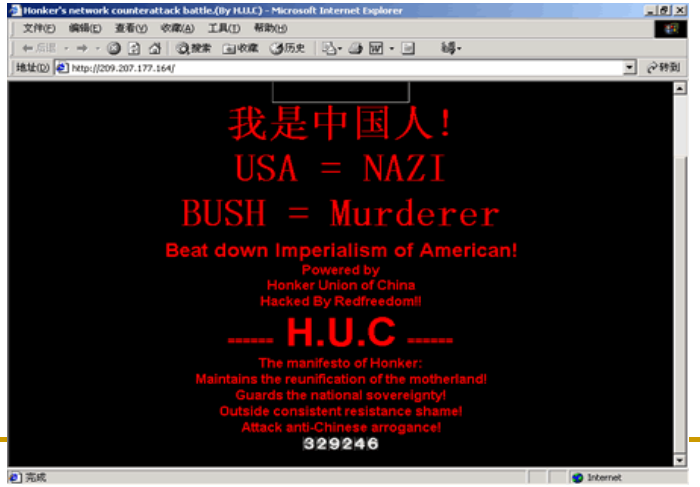
美国某大型商业网站

美国某政府网站



美国劳工部网站

美国某节点网站

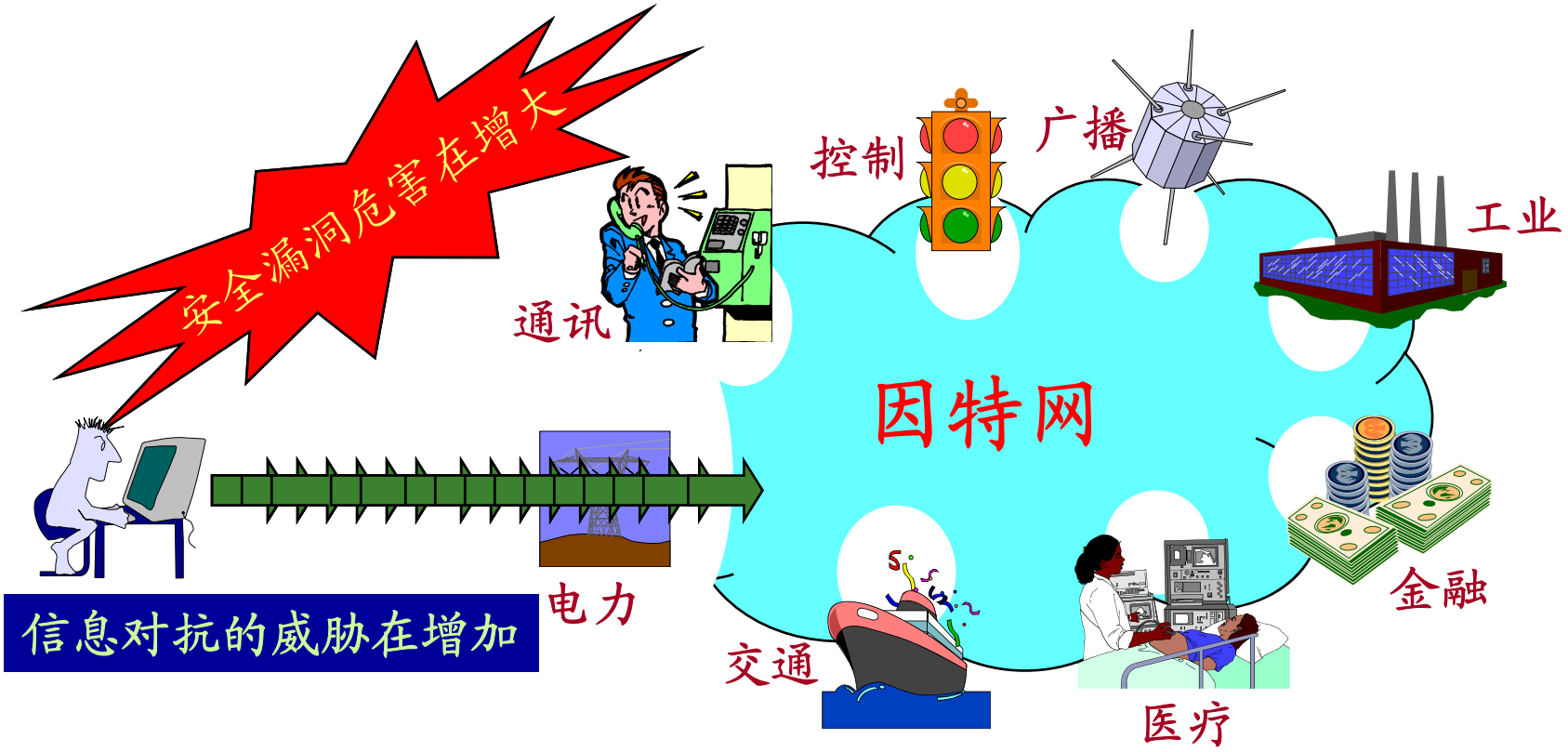


网络攻防概述

- 这次事件中被利用的典型漏洞(大部分都是NT/Win2000系统)
  - 用户名泄漏，缺省安装的系统用户名和密码
  - Unicode 编码可穿越firewall,执行黑客指令
  - ASP源代码泄露可远程连接的数据库用户名和密码
  - SQL server缺省安装
  - 微软Windows 2000登录验证机制可被绕过
  - Bind 远程溢出，Lion蠕虫
  - SUN rpc.sadmind 远程溢出，sadmin/IIS蠕虫
  - Wu-Ftpd 格式字符串错误远程安全漏洞
  - 拒绝服务 (syn-flood , ping)

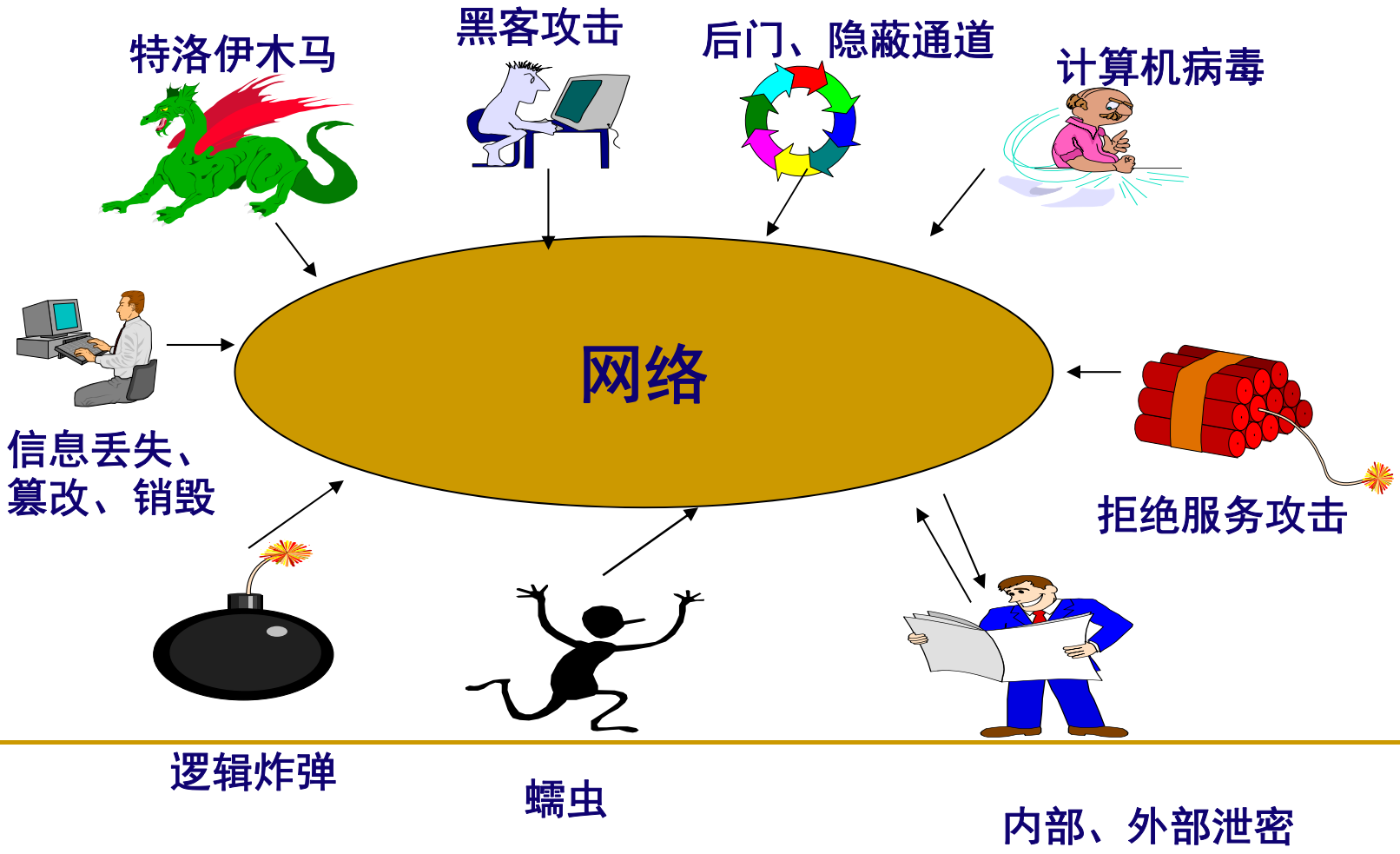
网络攻防概述

- 网络安全威胁国家基础设施



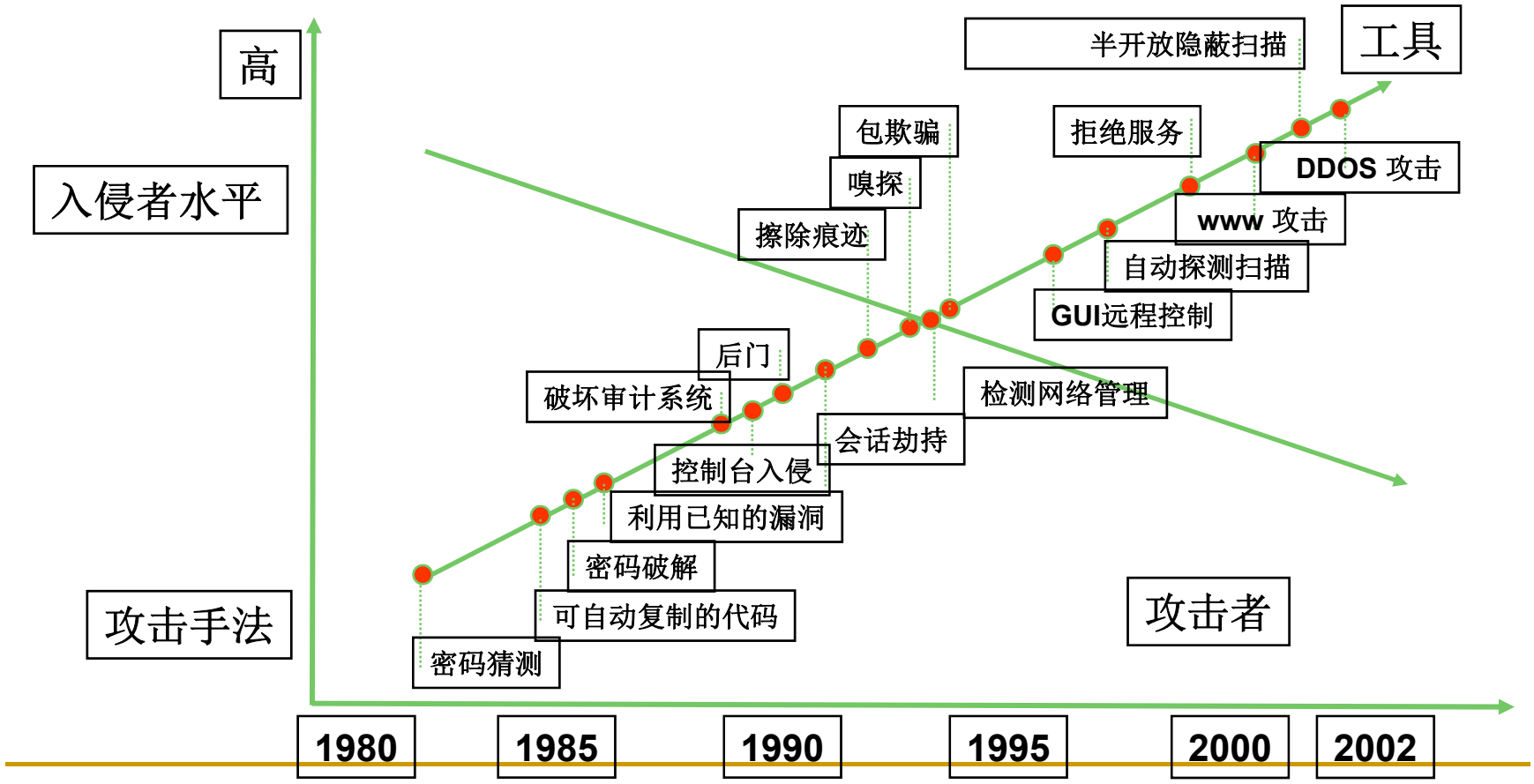
网络攻防概述

- 网络中存在的安全威胁



网络攻防概述

- 入侵技术的发展



网络攻防概述

- 黑客分类

白帽子创新者
- 设计新系统
- 打破常规
- 精研技术
- 勇于创新

没有最好，
只有更好

MS -Bill Gates
GNU -R.Stallman
Linux -Linus

灰帽子破解者
- 破解已有系统
- 发现问题/漏洞
- 突破极限/禁制
- 展现自我

计算机
为人民服务

漏洞发现 - Flashsky
软件破解 - 0 Day
工具提供 - Glacier

黑帽子破坏者
- 随意使用资源
- 恶意破坏
- 散播蠕虫病毒
- 商业间谍

人不为己，
天诛地灭

入侵者-K.米特尼克
CIH - 陈盈豪
攻击Yahoo者 -匿名

网络攻防概述

- 黑客文化
  - 常见替换
    - A = 4
    - B = 8
    - E = 3
    - G =9
    - I = 1
    - O = 0
    - S = 5
    - t = 7
    - Z = 2

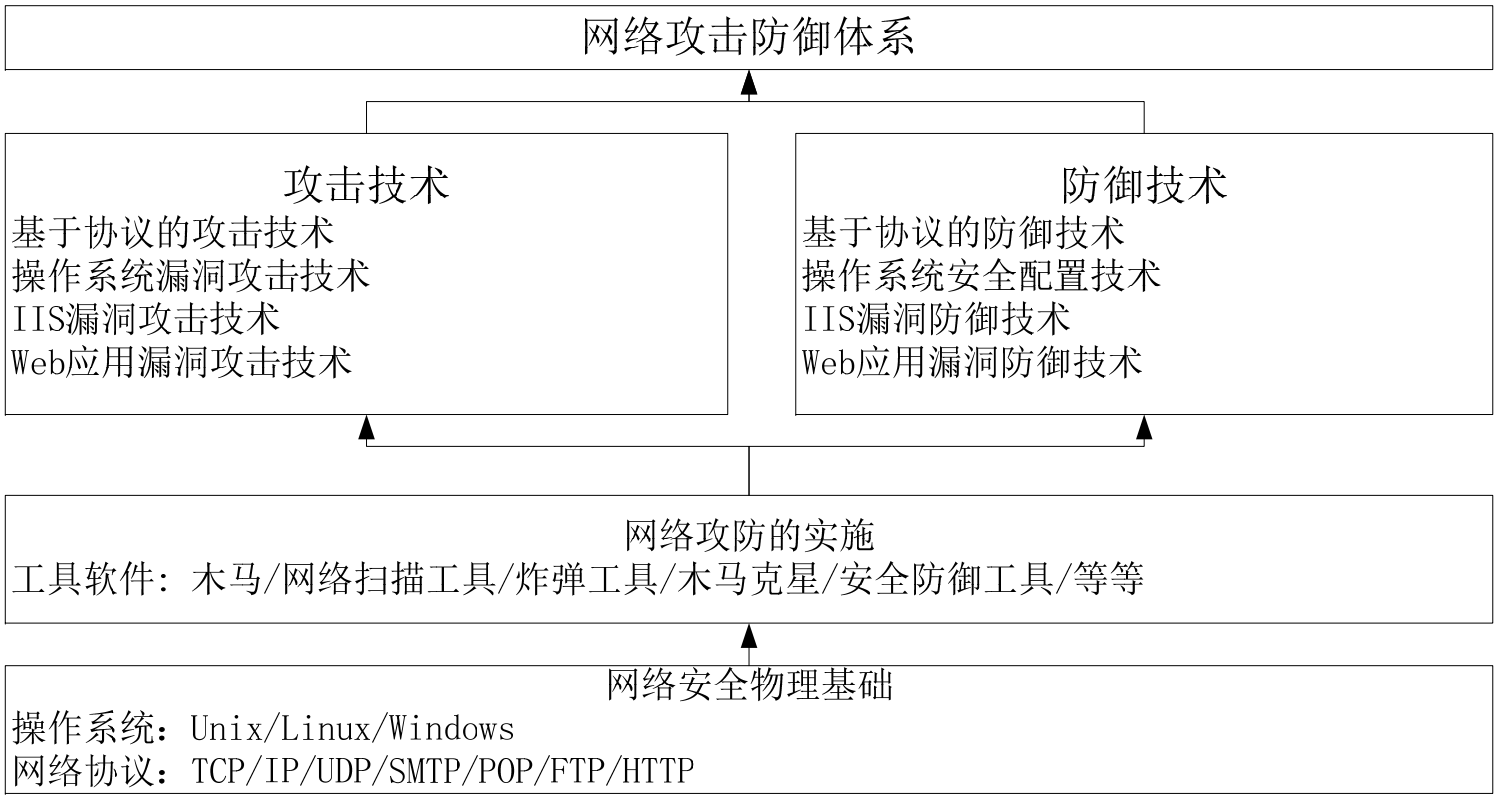
H4x3r 14n9u493 i5 4 diff3r3n7 14n9u493 fr0m 3n91i5h.

w3 c4n find 7hi5 14n9u493 in h4x3r'5 885, IRC 0r 07h3r Ch477in9 p14c3.

  - 常见缩写
    - CK = x
    - You = u
    - Are = r
    - See = c
    - And = n / &
    - Not = !

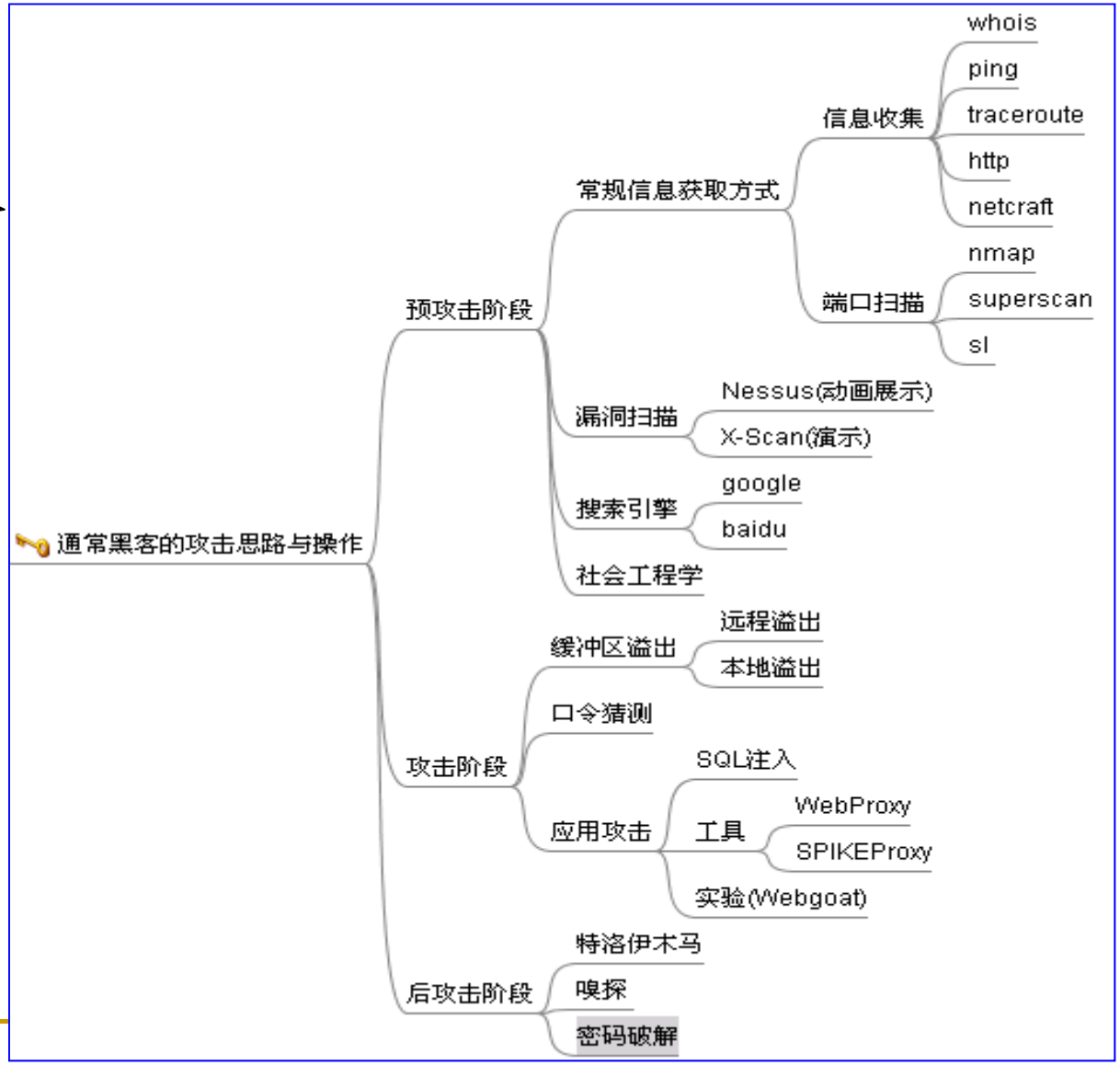
网络攻防概述

- 网络攻击防御体系



网络攻防概述

- 网络攻击步骤



目录

- 网络攻防概述
- 安全攻防案例分析
- 常见网络安全技术

安全攻防案例分析

- 当前黑客与网络安全事件的特点
  - 黑客可以轻易地施行跨网、跨国攻击
    - 攻击、入侵工具和工具包数量大量增加，可轻易从互联网上获取，使用操作更加简单方便
    - 具有安全知识和“专业”的人员的数量在增加
  - 复合趋势
    - 黑客、病毒和垃圾邮件技术整合在一个蠕虫当中
    - 黑客组合攻击开始出现
  - 攻击往往通过一级或者多级跳板进行
    - 黑客技术水平在增强
    - 有组织、有计划犯罪事件再增加，防止追查

安全攻防案例分析

- 当前黑客与网络安全事件的特点
  - 大规模事件出现日益频繁
    - 大规模网络蠕虫事件（“冲击波”、“震荡波”、红色代码F变种等）
    - 大量垃圾邮件的出现
  - 传播速度越来越快
    - 利用系统漏洞，进行自动扫描
    - 由于浏览网页或查看E-Mail而受到感染或攻击
    - DDoS攻击

安全攻防案例分析

- 当前黑客与网络安全事件的特点
  - 对终端的攻击比率越来越高
    - 网上游戏、网上银行和电子商务的增加
    - 针对终端设计的黑客工具和木马
    - 补丁与升级不够及时
    - 缺乏安全防范意识
  - 攻击事件的破坏程度在增加

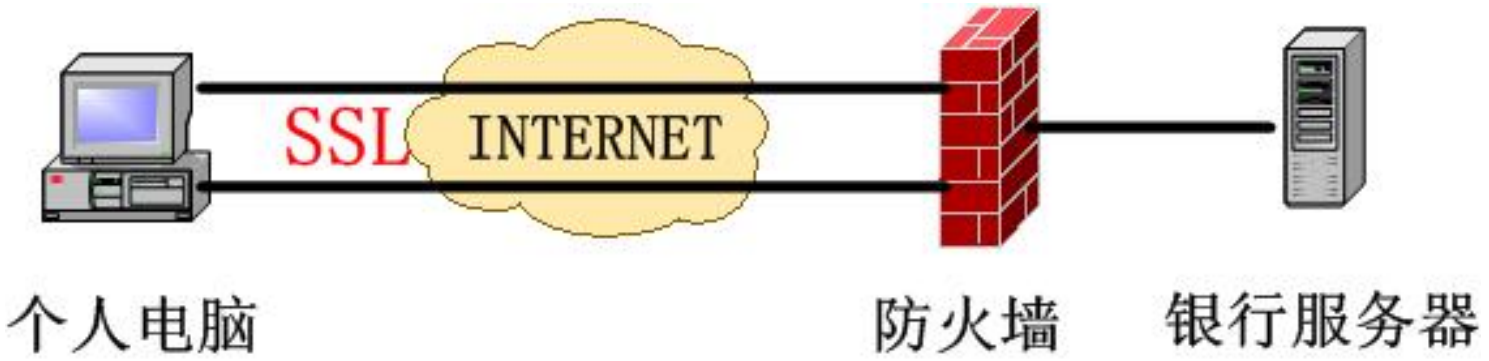
安全攻防案例分析

- 典型网络安全案件分析
  - 木马与“网银大盗”
    - 冰河：国产木马，有G_Client.exe,G_server.exe二个文件

客户端界面

安全攻防案例分析

- 典型网络安全案件分析
  - 木马与“网银大盗”
    - “网银大盗”



网上银行架构

安全攻防案例分析

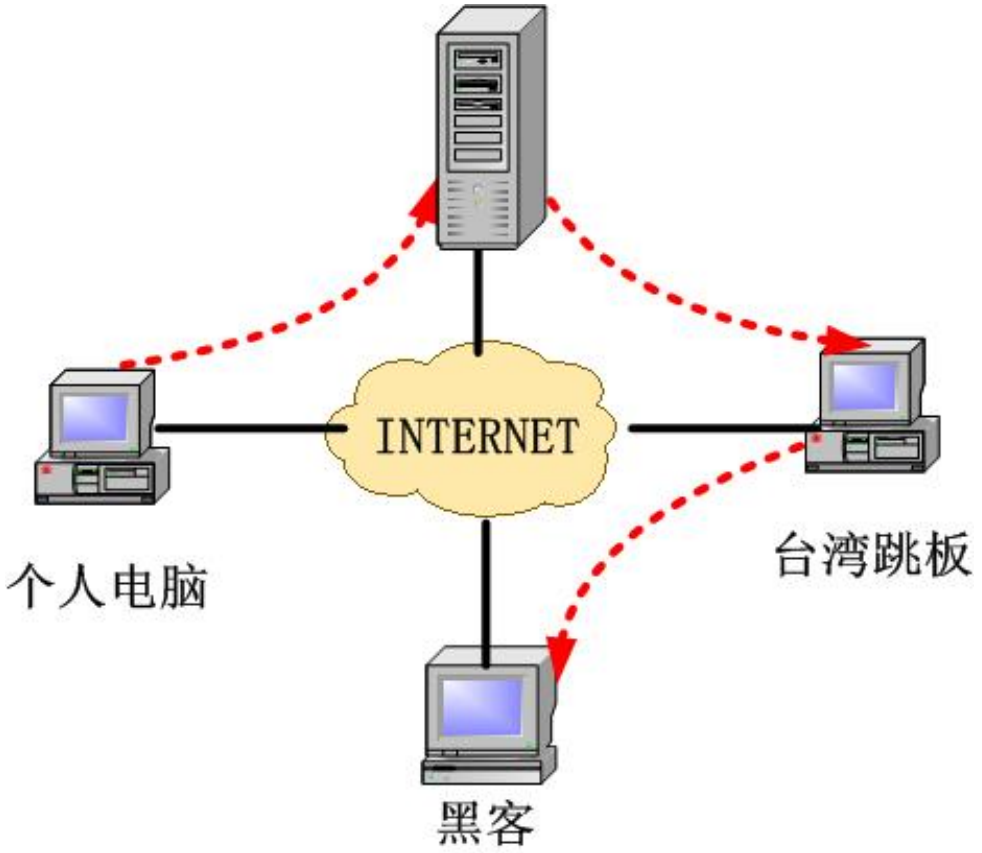
- 典型网络安全案件分析
  - 木马与“网银大盗”
    - 网银大盗II(Troj_Dingxa.A)
      - 现象
        - 盗取网上银行的帐号、密码、验证码等。
      - 生成文件：%System%下，svch0st.exe
      - 修改注册表:
        HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run下创建:
        "svch0st.exe" = "%System%\svch0st.exe"
        "taskmgr.exe" = "%System%\svch0st.exe"

安全攻防案例分析

- 典型网络安全案件分析
  - 木马与“网银大盗”
    - 网银大盗II(Troj_Dingxa.A)
      - 原理
        - 木马程序，非主动传播，主要通过用户在浏览某些网页或点击一些不明连接及打开不明邮件附件等操作时，间接感染用户电脑
      - 解决办法
        - 1、终止病毒进程"svch0st.exe"
        - 2、注册表修复
        - 3、删除病毒释放的文件"svch0st.exe"
        - 4、配置防火墙和边界路由器

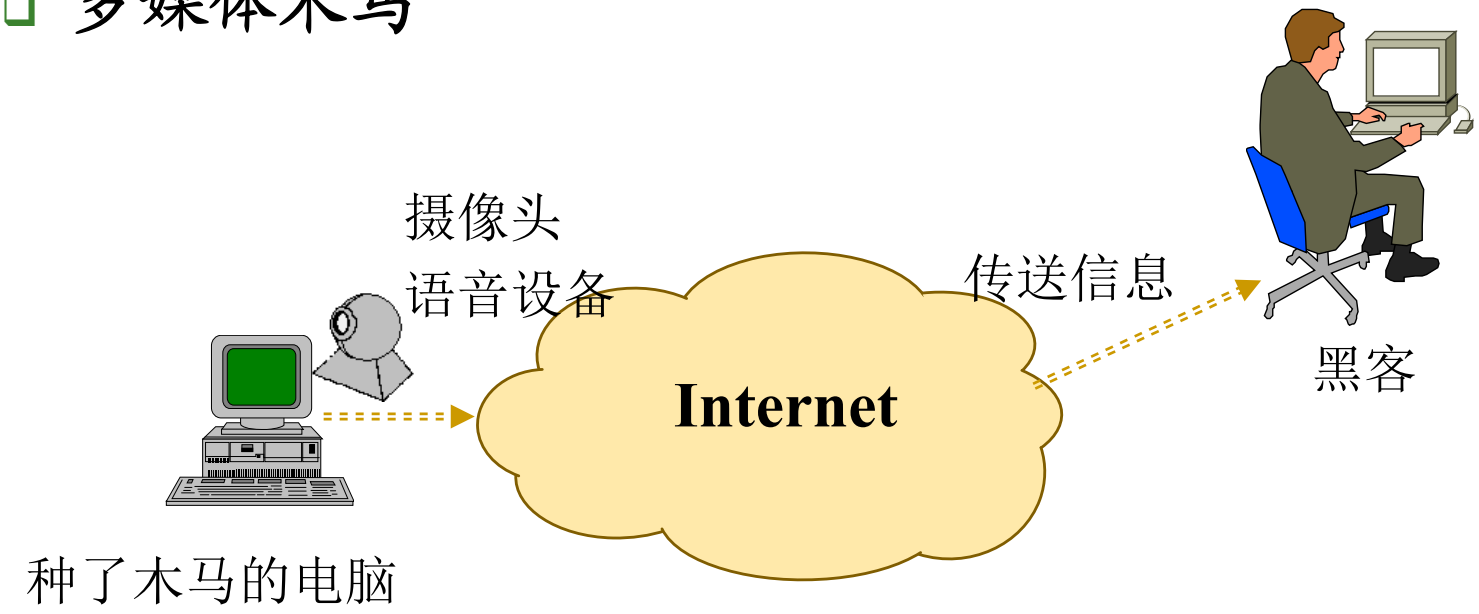
安全攻防案例分析

- 典型网络安全案件分析
  - “网银大盗”案例



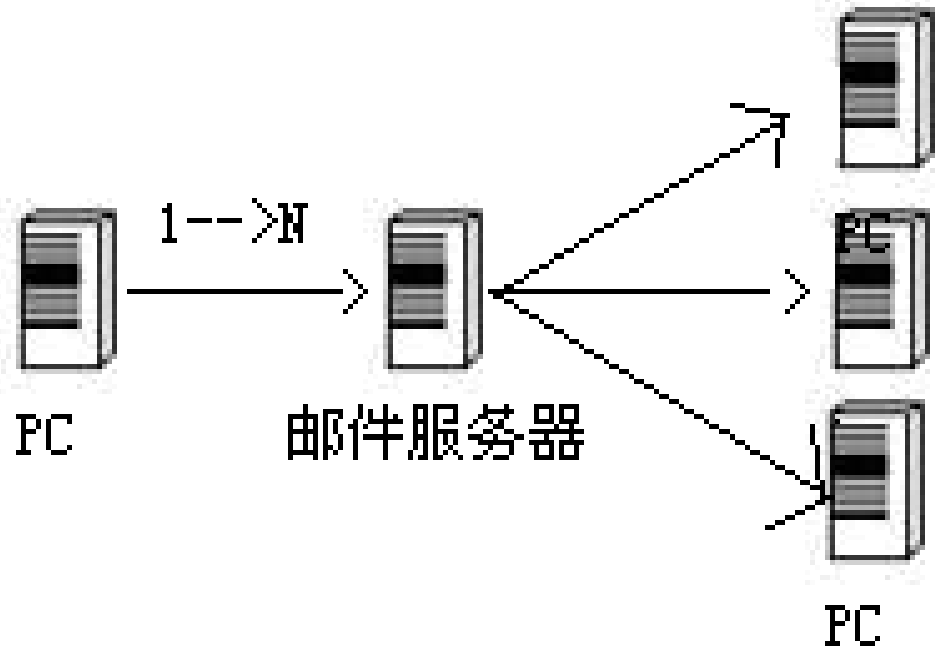
安全攻防案例分析

- 典型网络安全案件分析
  - 多媒体木马



安全攻防案例分析

- 典型网络安全案件分析
  - 匿名电子邮件转发
    - 漏洞名称：Exchange Server匿名转发漏洞

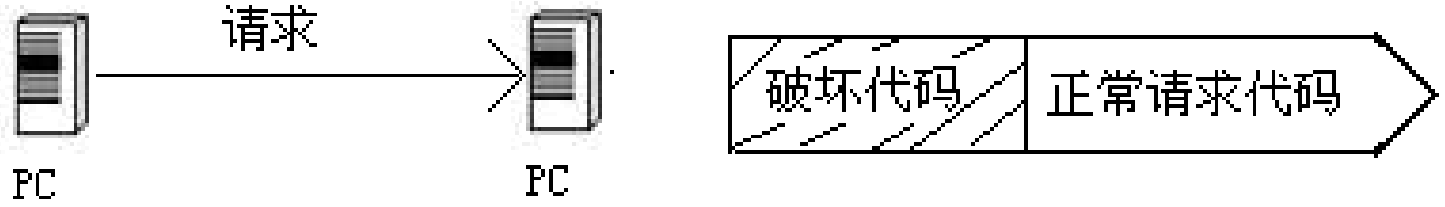


安全攻防案例分析

- 典型网络安全案件分析
  - 匿名电子邮件转发
    - 造成危害
      - 网络堵塞
      - 被用于反动宣传
      - 正常邮件服务器被RBL组织封闭
    - 解决方法
      - 打补丁
      - 关闭该服务或端口25 , 110

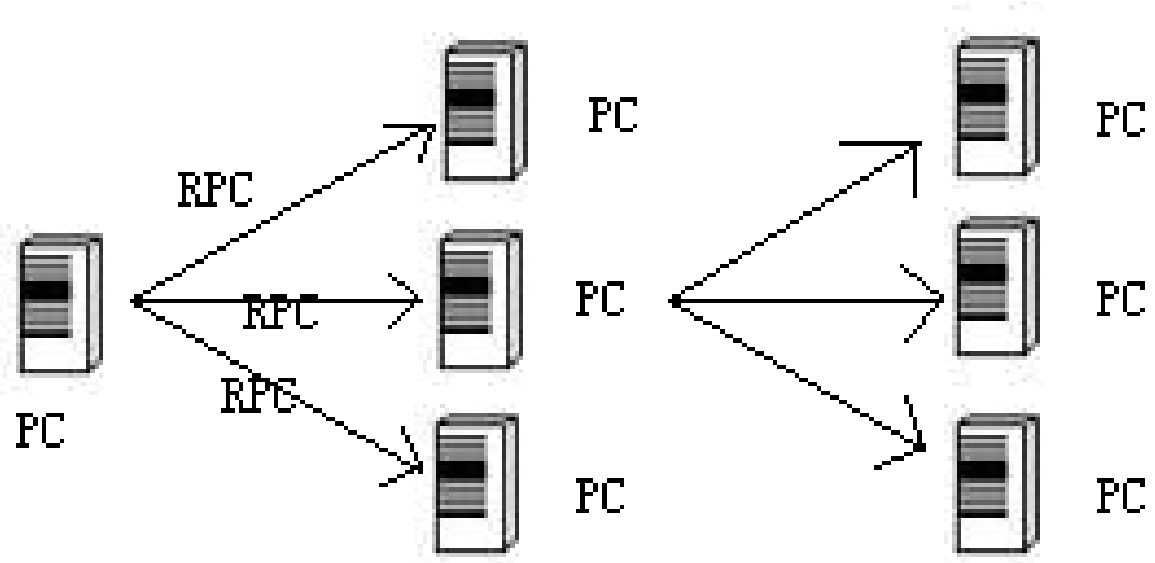
安全攻防案例分析

- 典型网络安全案件分析
  - 溢出攻击与DCOM RPC漏洞
    - 攻击原理



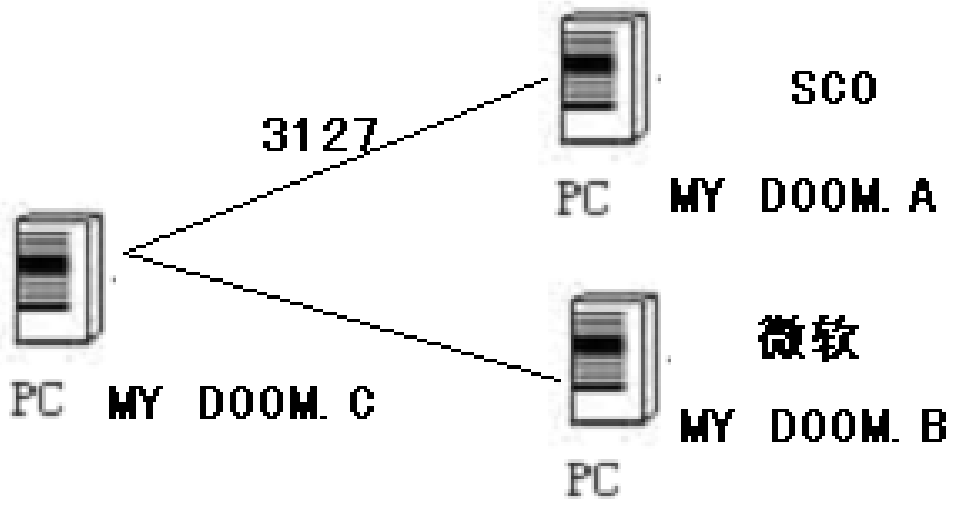
安全攻防案例分析

- 典型网络安全案件分析
  - 溢出攻击与DCOM RPC漏洞
    - 造成的危害---冲击波



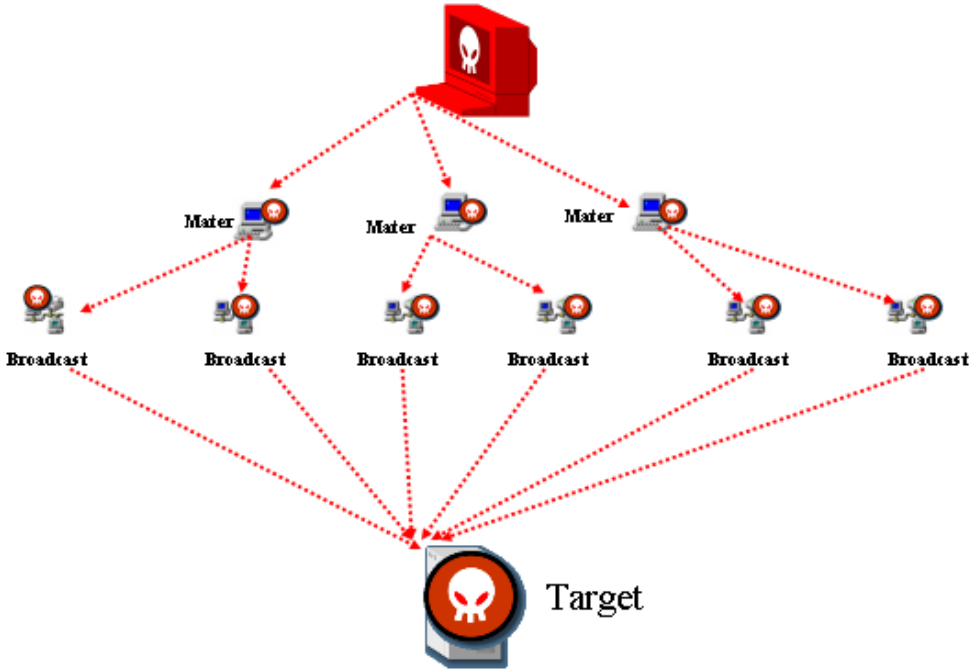
安全攻防案例分析

- 典型网络安全案件分析
  - MY DOOM案例分析： 邮件蠕虫:MY DOOM
    - 现象
      - 通过电子邮件附件传播，设定向www.sco.com和www.microsoft.com 发起DDoS攻击
    - 原理



安全攻防案例分析

- 典型网络安全案件分析
  - DDoS攻击
    - 所谓的DDoS攻击——一群“恶意访问”、“堵店门”、“占空间”、还“调戏店员”的非法流量



安全攻防案例分析

- 典型网络安全案件分析
  - DDoS攻击
    - DDoS攻击方法
      - 死亡之ping（ping of death）
      - 泪滴（teardrop）
      - UDP洪水（UDP flood）
      - SYN洪水（SYN flood）
      - Land攻击
      - Smurf攻击
      - Fraggle攻击

安全攻防案例分析

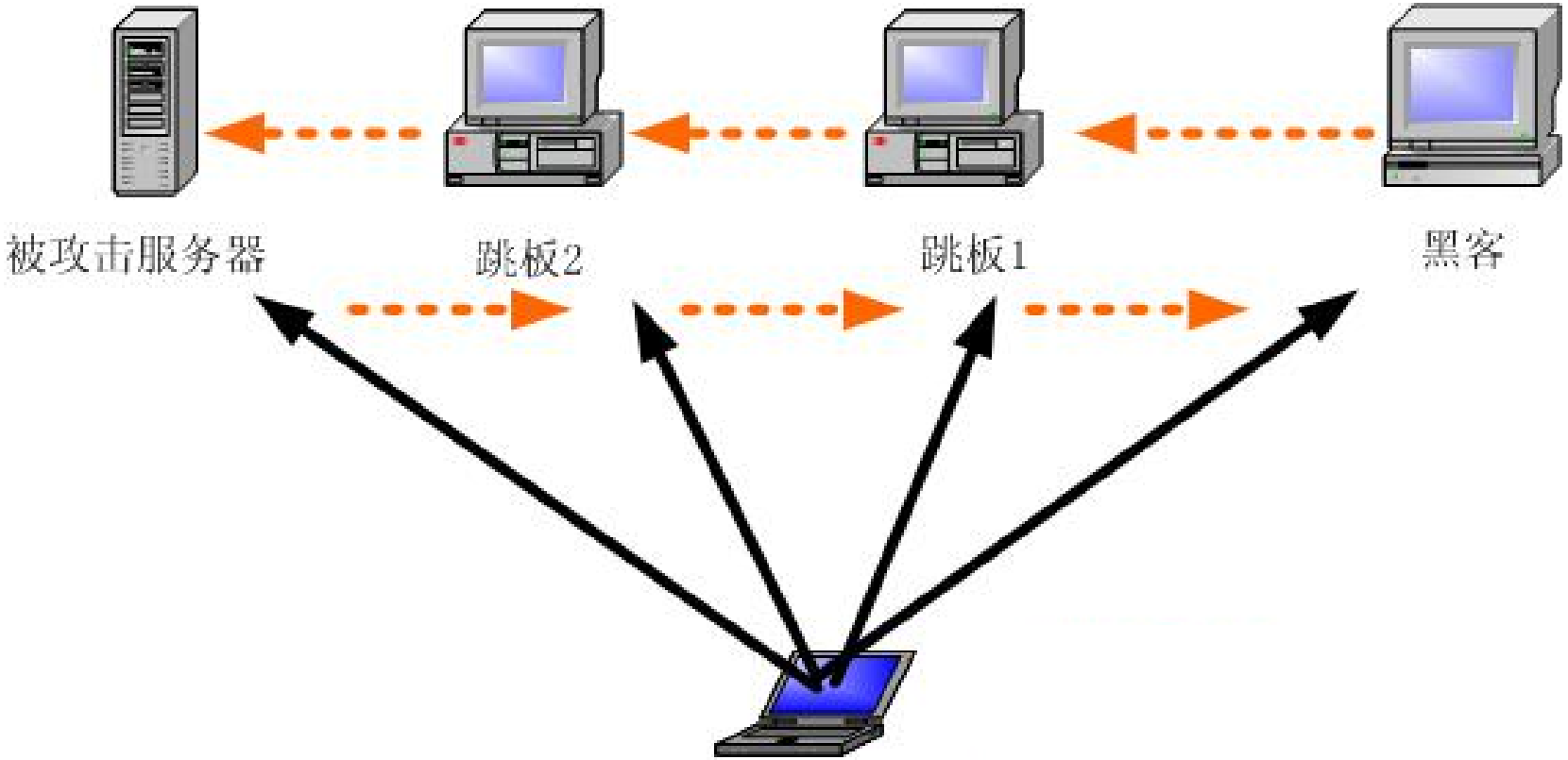
- 典型网络安全案件分析
  - DDoS攻击
    - 常用DDoS攻击工具
      - Thankgod
      - SYN Flooder
      - 独裁者
      - Trinoo
      - TFN2K
      - Stacheldraht

目录

- 网络攻防概述
- 安全攻防案例分析
- 常见网络安全技术

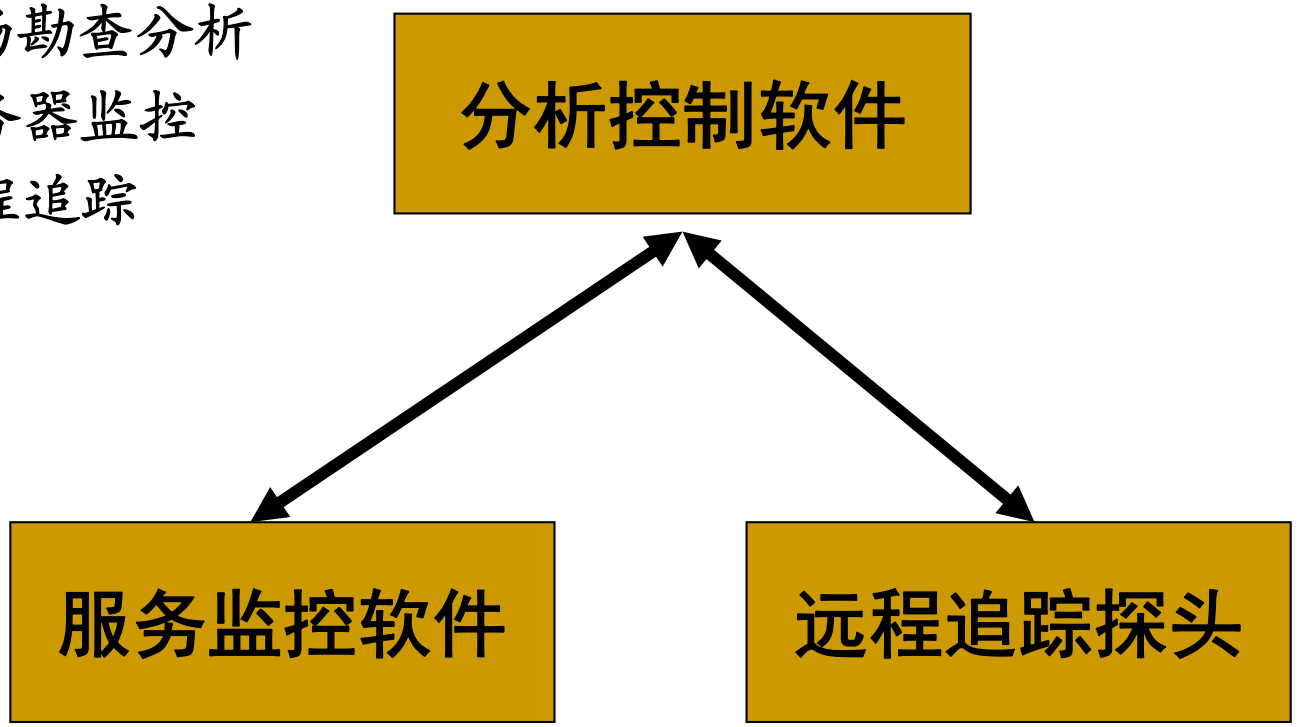
常见网络安全技术

- 黑客侦查与追踪系统



常见网络安全技术

- 黑客侦查与追踪系统
  - 系统组成
    - 1、现场勘查分析
    - 2、服务器监控
    - 3、远程追踪



常见网络安全技术

- DDoS攻击防御技术
  - 当前DDoS防御技术
    - SYN代理
    - SYN网关
  - DDoS防御网关

常见网络安全技术

- 应用层攻击防御
  - Web风险的产生

风险的产生

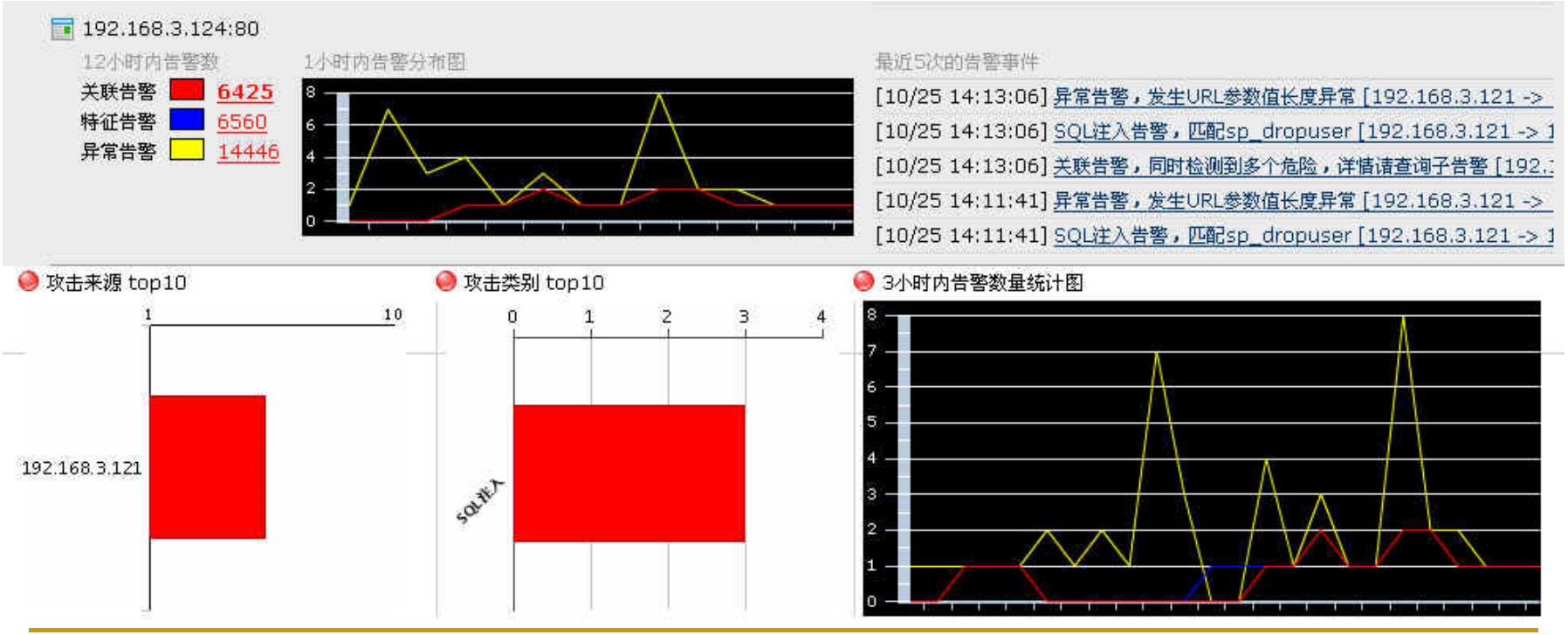
- 80%基于WEB的应用或多或少都存在安全问题，其中很大一部分是相当严重的问题
- 防火墙、IDS或者使用SSL协议对此毫无用处
- 不仅仅是开放在Internet的Web存在风险
- 更多的 ERP/CRM/MSS 系统也都使用了Web应用程序
- ……

攻击结果

- 泄漏客户敏感数据，例如网银账号，手机通话记录等。
- 篡改数据，发布虚假信息或者进行交易欺诈。
- 使WEB网站成为钓鱼攻击的平台，将攻击扩大到所有访问WEB应用的用户。例如：网银成为了钓鱼的场所，那么其危害和影响是不言而喻的。
- 拒绝服务，利用应用的弱点，造成拒绝服务，影响业务的正常运作

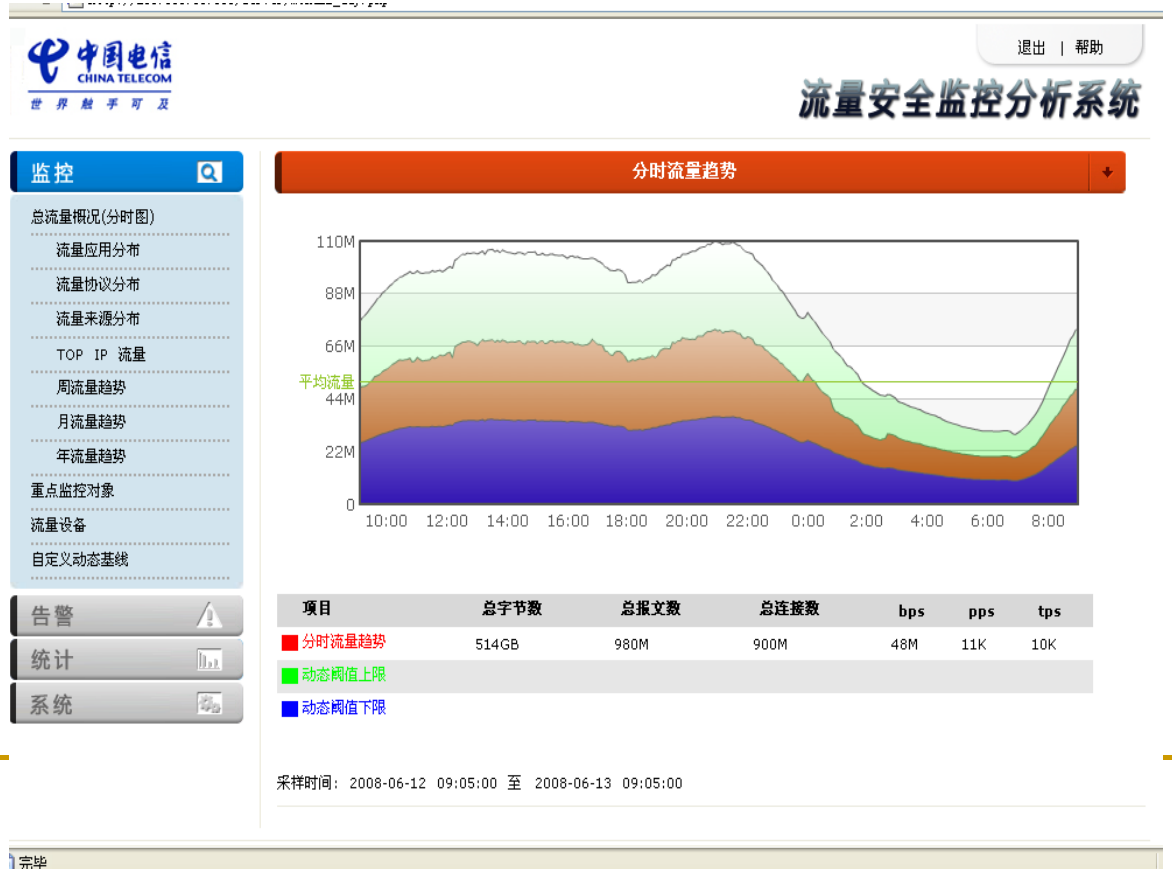
常见网络安全技术

- **WEB应用深度防御**
  - 实时告警



常见网络安全技术

- 日常安全维护
  - 建立整体监控管理系统



常见网络安全技术

- 日常安全维护
  - 定期备份数据库和供下载的文档
    - 定期备份数据库和上传的文件，不要怕麻烦，这个制度很有必要

常见网络安全技术

- 日常安全维护
  - 掌握最新的补丁以及漏洞信息
    - 经常关注官方网站的补丁发布，及时修改。

常见网络安全技术

- 日常安全维护
  - 设置足够强壮的密码
    - 要保证密码是“健壮的”，即不能像“123456”这样容易猜测，必须是数字、字母和符号的组合。这点很重要，不然所有的安全措施都是徒劳！

常见网络安全技术

- **Windows系统安全加固**
  - 使用Windows update安装最新补丁;
  - 更改密码长度最小值、密码最长存留期、密码最短存留期、帐号锁定计数器、帐户锁定时间、帐户锁定阀值，保障帐号以及口令的安全;
  - 卸载不需要的服务;
  - 将暂时不需要开放的服务停止;
  - 限制特定执行文件的权限;
  - 设置主机审核策略;
  - 调整事件日志的大小、覆盖策略;
  - 禁止匿名用户连接;
  - 删除主机管理共享;
  - 限制Guest用户权限;
  - 安装防病毒软件、及时更新病毒代码库;
  - 安装个人防火墙

常见网络安全技术

安全解决方案