

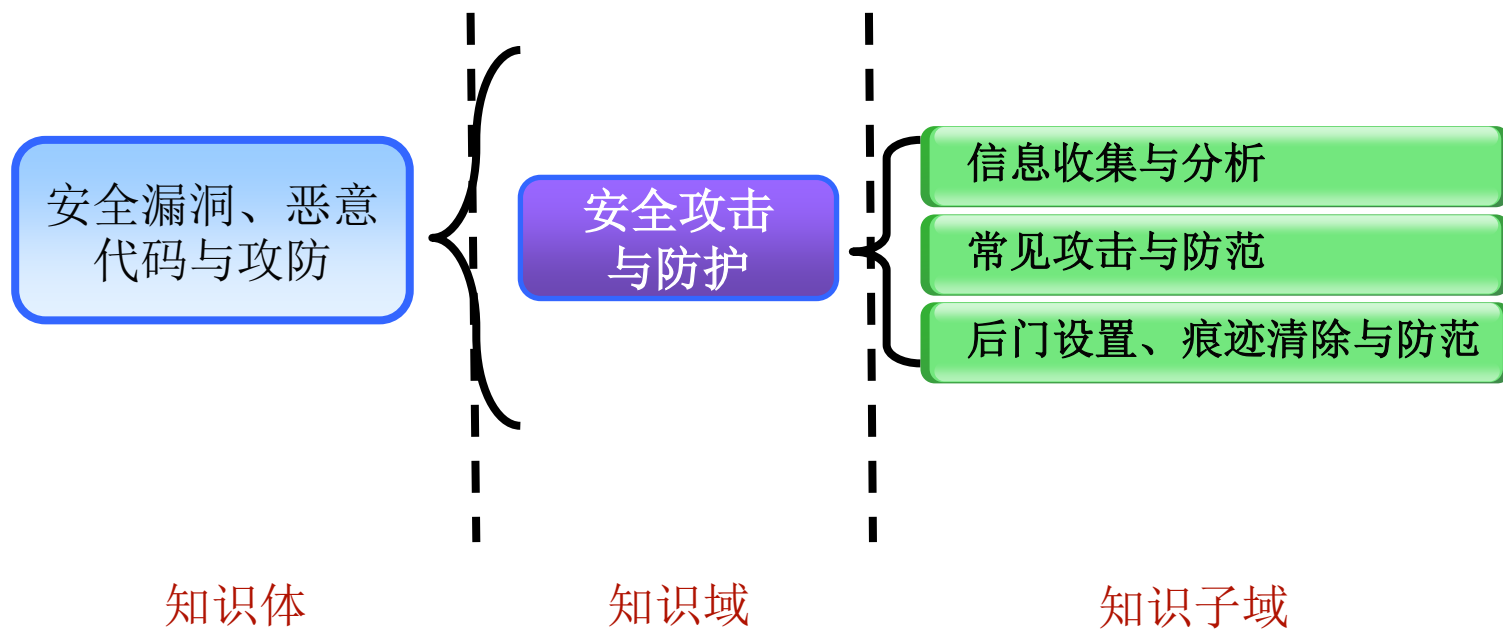
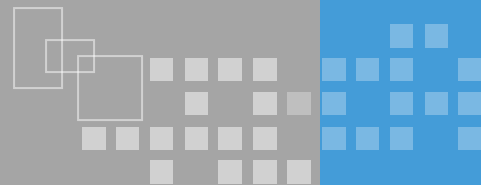


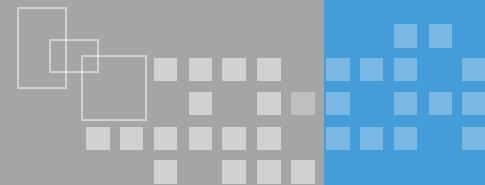
# 安全攻击与防护

中国信息安全测评中心



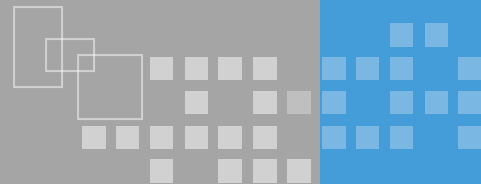
# 课程内容





## ❖ 知识子域：信息收集与分析

- 了解信息收集与分析的作用
- 理解快速定位、定点挖掘、漏洞查询等信息收集与分析的方法
- 理解信息收集与分析的防范措施



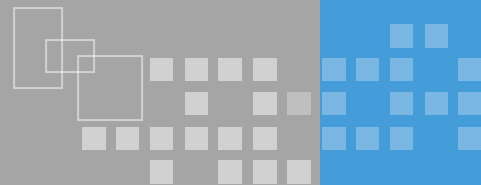
## ❖ 攻击的过程

- 信息收集
- 目标分析
- 实施攻击
- 方便再次进入
- 打扫战场

## ❖ 防护

- 针对以上提到的行为了解其原理并考虑应对措施






## ❖ 为什么要收集信息

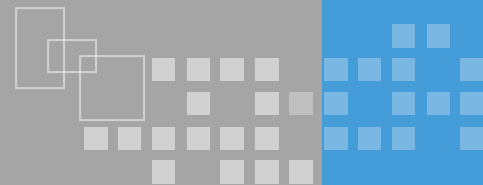
- 获取攻击目标大概信息
- 为下一步攻击做准备
- 利用收集的信息直接攻击

## ❖ 为什么需要分析目标

- 确定收集信息的准确性
- 去除迷惑信息（例如：index.ycs是java开发，开发人员修改了脚本后缀以迷惑攻击者）
- 攻击方式及攻击路径的选择



知己知  
彼，百  
战不殆

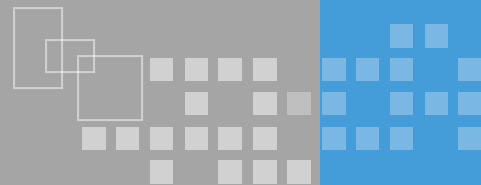


## ❖ 为什么需要分析目标

- 确定收集信息的准确性
- 去除迷惑信息（例如：index. ycs是java开发，开发人员修改了脚本后缀以迷惑攻击者）
- 攻击方式及攻击路径的选择

## ❖ 分析目标的方式

- 漏洞扫描
- 漏洞库
- 论坛等交互应用
- .....



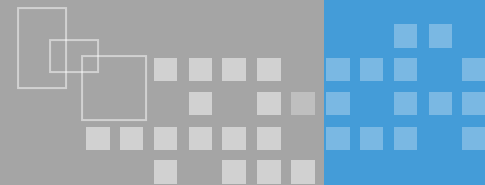
## ❖ 现实中的范例：著名的照片泄密案

### ■ 背景

- 大庆油田在发现之初，其位置、储量、产量等信息全部定为国家机密
- 1964年《中国画报》封面泄露信息
  - 衣着判断→北纬46度至48度的区域（即齐齐哈尔与哈尔滨之间）
  - 所握手柄的架式→油井的直径
  - 钻井与背后油田的距离和井架密度→储量和产量



设计出适合中国大庆的设备，在我国设备采购中中标！



## ❖ 微博时代的范例：影星的住址

### ■ 背景：

- 明星家庭住址是明星隐私，她们都不愿意透露，微博时代，明星也爱玩微博

### ■ 微博信息

- 13:50:四环堵死了，我联排要迟到了？
- 在北京工作这么久，都没在北京中心地带买一套房子
- 光顾着看围脖，忘记给老爸指路，都开到中关村了

### ■ 结论：北四环外某个成熟小区，小区中间有三个相连的方形花坛

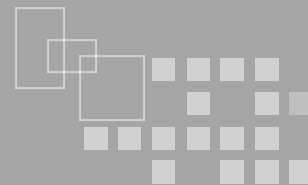
### ■ Google earth能帮助我们快速找到这个小区



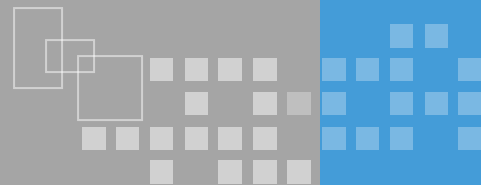




# 收集哪些信息



- ❖ 目标系统的信息系统相关资料
  - 域名、网络拓扑、操作系统、应用软件
  - 相关脆弱性
- ❖ 目标系统的组织相关资料
  - 组织架构及关联组织
  - 地理位置细节
  - 电话号码、邮件等联系方式
  - 近期重大事件
  - 员工简历
- ❖ 其他可能令攻击者感兴趣的任何信息



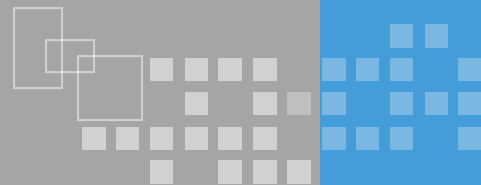
## ❖ 快速定位

- Google 搜索 “5sf67.jsp” 可以找到存在此脚本的Web网站
- Google 搜索 “teweb/default.htm” 就可找到开放着远程Web连接的服务器

## ❖ 信息挖掘

- 定点采集
  - Google 搜索 “.doc+website” 挖掘信息
- 隐藏信息
  - .mdb、.ini、.txt、.old、.bak、.001……
- 后台入口





## ❖ Whois

- Whois是一个标准服务，可以用来查询域名是否被注册以及注册的详细资料
- Whois 可以查询到的信息
  - 域名所有者
  - 域名及IP地址对应信息
  - 联系方式
  - 域名到期日期
  - 域名注册日期
  - 域名所使用的 DNS Servers
  - .....

### Administrative Contact:

Xinpu Wang  
Baidu Online Network Technology Co.Ltd  
3F Baidu Campus No.10 Shangdi 10th Street Haidian District  
Beijing Beijing 100085  
CN

domainmaster@baidu.com +86.1059926607 Fax: +86.1059920061

### Technical Contact, Zone Contact:

Xinpu Wang  
Baidu Online Network Technology Co.Ltd  
3F Baidu Campus No.10 Shangdi 10th Street Haidian District  
Beijing Beijing 100085  
CN

domainmaster@baidu.com +86.1059926607 Fax: +86.1059920061

Created on.....: 1999-10-11.

Expires on.....: 2015-10-11.

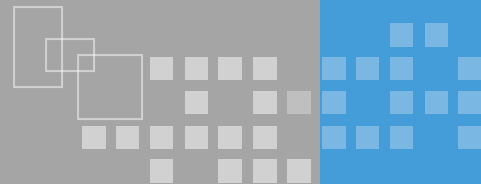
Record last updated on..: 2010-10-27.

### Domain servers in listed order:

ns3.baidu.com  
dns.baidu.com  
ns4.baidu.com  
ns2.baidu.com



# 信息收集技术-域名与IP查询



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.0.6002]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>nslookup www.baidu.com
服务器:  gjjline.bta.net.cn
Address:  202.106.0.20

非权威应答:
名称:    www.a.shifen.com
Addresses: 61.135.169.125
          61.135.169.105
Aliases:  www.baidu.com

C:\Users\Administrator>
```

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.0.6002]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [61.135.169.105] 具有 32 字节的数据:
来自 61.135.169.105 的回复: 字节=32 时间=19ms TTL=56
来自 61.135.169.105 的回复: 字节=32 时间=18ms TTL=56
来自 61.135.169.105 的回复: 字节=32 时间=18ms TTL=56
来自 61.135.169.105 的回复: 字节=32 时间=18ms TTL=56

61.135.169.105 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 18ms, 最长 = 19ms, 平均 = 18ms

C:\Users\Administrator>
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\shencn>tracert www.cisphome.cn

通过最多 30 个跃点跟踪
到 www.cisphome.cn [112.125.37.6] 的路由:

 1  5 ms    3 ms    3 ms  shencn-PC [192.168.1.11]
 2  20 ms   19 ms   17 ms  221.222.216.1
 3  17 ms   18 ms   16 ms  61.148.162.157
 4  18 ms   17 ms   19 ms  124.65.61.129
 5  19 ms   15 ms   17 ms  61.148.3.34
 6  24 ms   19 ms   20 ms  202.106.43.142
 7  21 ms   19 ms   17 ms  182.92.255.228
 8  *      *      *      请求超时。
 9  *      *      *      请求超时。
10 18 ms   17 ms   19 ms  112.125.37.6
```

## ❖ 域名与IP查询— nslookup

- 操作系统自带命令，主要是用来查询域名名称和 IP 之间的对应关系

## ❖ 网络状况查询— Ping

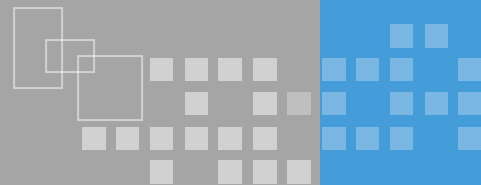
- 系统自带命令，测试与远端电脑或网络设备的连接状况

## ❖ 网络路径状况查询— tracert

- 系统自带命令，测试与远端电脑或网络设备之间的路径



# 系统信息收集-服务旗标检测



C:\WINDOWS\system32\cmd.exe

220 Serv-U FTP Server v6.0 for WinSock ready...

quit

221 Goodbye!

FTP回显  
信息

C:\WINDOWS\system32\cmd.exe

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

Not Implemented</title>

</head><body>

<h1>Method Not Implemen

dex.htm not supported.<br />

</p>

<hr>

<address>Apache/2.0.59 (Win32) mod\_jk/1.2.23

Server at eservice. [REDACTED] gov.cn Port 80</address>

</body></html>

Web回显信息

失去了跟主机的连接。



# 系统及应用信息收集-TCP/IP协议栈检测

## ❖ 原理

- 不同厂商对IP协议栈实现之间存在许多细微的差别，通过这些差别就能对目标系统的操作系统加以猜测。

## ❖ 检测方法

- 主动检测
- 被动检测

```
C:\Windows\system32\cmd.exe

C:\Users\shencn>ping www.sina.com.cn

正在 Ping polaris.sina.com.cn [202.108.33.60] 具有 32 字节
来自 202.108.33.60 的回复: 字节=32 时间=18ms TTL=249
来自 202.108.33.60 的回复: 字节=32 时间=16ms TTL=249
来自 202.108.33.60 的回复: 字节=32 时间=16ms TTL=249
来自 202.108.33.60 的回复: 字节=32 时间=18ms TTL=249

202.108.33.60 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 16ms, 最长 = 18ms, 平均 = 17ms

C:\Users\shencn>ping www.163.com

正在 Ping 163.xdwscache.glb0.lxdns.com [123.126.72.30] 具
来自 123.126.72.30 的回复: 字节=32 时间=19ms TTL=55
来自 123.126.72.30 的回复: 字节=32 时间=18ms TTL=55
来自 123.126.72.30 的回复: 字节=32 时间=22ms TTL=55
来自 123.126.72.30 的回复: 字节=32 时间=20ms TTL=55

123.126.72.30 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 18ms, 最长 = 22ms, 平均 = 19ms

C:\Users\shencn>
```

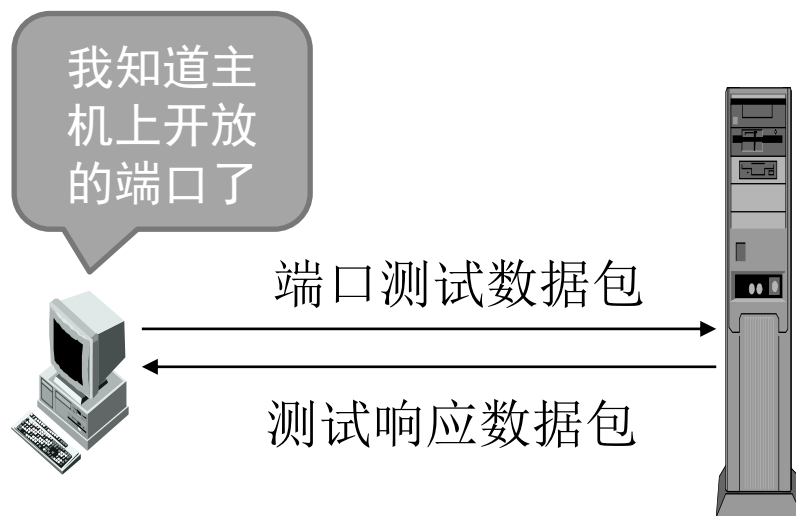


## ❖ 原理

- 通过端口扫描确定主机开放的端口，不同的端口对应运行着的不同的网络服务

## ❖ 扫描方式

- 全扫描
- 半打开扫描
- 隐秘扫描
- 漏洞扫描
- .....





# 工具介绍-端口扫描

## ❖ Nmap

### ■ 简介

- 被称为
- 有for U
- 需要Lib
- 能够进行

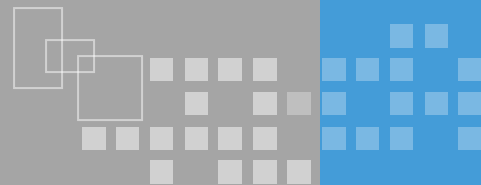
### ■ 使用

- -sS: 半
- -sU: ud
- -O: 操作
- -P0: 强
- -p: 指定
- -v: 详细

```
命令提示符
D:\nmap-3.00\nmap-3.00>nmap -sS -v -O 192.168.102.177

Starting nmap U. 3.00 ( www.insecure.org/nmap )
Host HERO (192.168.102.177) appears to be up ... good.
Initiating SYN Stealth Scan against HERO (192.168.102.177)
Adding open port 139/tcp
Adding open port 445/tcp
Adding open port 3372/tcp
Adding open port 2105/tcp
Adding open port 1026/tcp
Adding open port 1025/tcp
Adding open port 135/tcp
The SYN Stealth Scan took 1 second to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are f
irewalled
For OSScan assuming that port 135 is open and port 1 is closed and neither are f
irewalled
For OSScan assuming that port 135 is open and port 1 is closed and neither are f
irewalled
Interesting ports on HERO (192.168.102.177):
(The 1594 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
445/tcp    open       microsoft-ds
1025/tcp   open       NFS-or-IIS
1026/tcp   open       LSA-or-nterm
2105/tcp   open       eklogin
3372/tcp   open       msdtc
No exact OS matches for host (If you know what OS is running on it, see http://w
ww.insecure.org/cgi-bin/nmap-submit.cgi).
```





## ❖ 原理

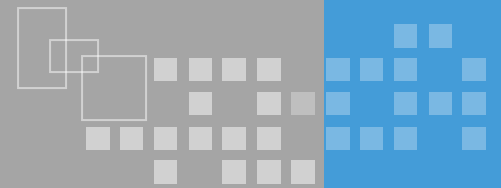
- 向目标发送各类测试报文，根据目标主机反馈情况判断是否存在或可能存在某种类型的漏洞

## ❖ 意义

- 进行网络安全评估
- 为网络系统的加固提供先期准备
- 被网络攻击者加以利用来获取重要的数据信息



# 漏洞扫描工具



## ❖ 网络设备漏洞扫描器

- Cisco Auditing Tools

## ❖ 集成化的漏洞扫描器

- Nessus
- Shadow Security Scanner
- eEye的Retina
- Internet Security Scanner
- GFI LANguard

## ❖ 专业web扫描软件

- IBM appscan
- Acunetix Web Vulnerability

## ❖ 数据库漏洞扫描器

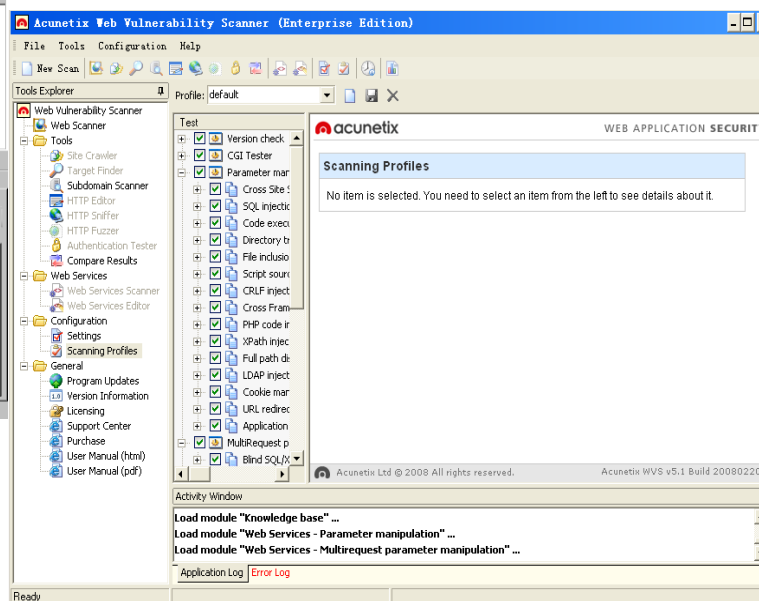
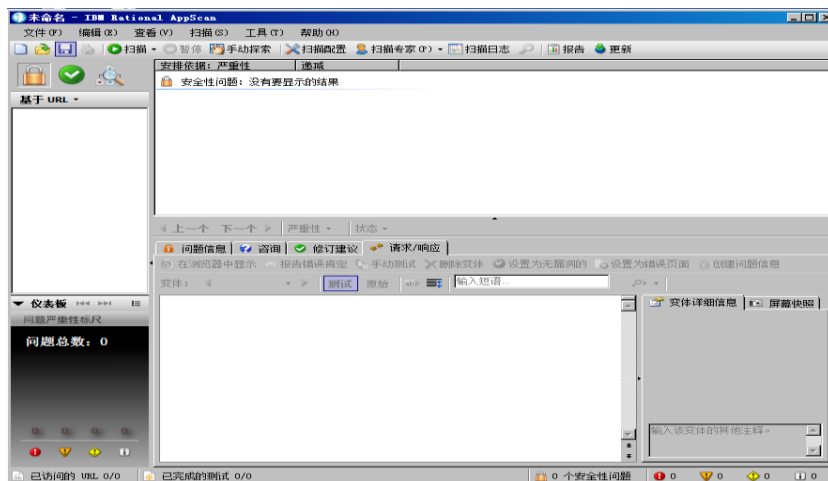
- ISS Database Scanner
- oscanner Oracle数据库扫描器
- Metacoretex                      数据安全审计工具



# 工具介绍-web安全扫描

❖ IBM AppScan

❖ Acunetix Web Vulnerability Scanner





# 工具介绍-漏洞扫描

## ❖ Nessus

### ■ 构架

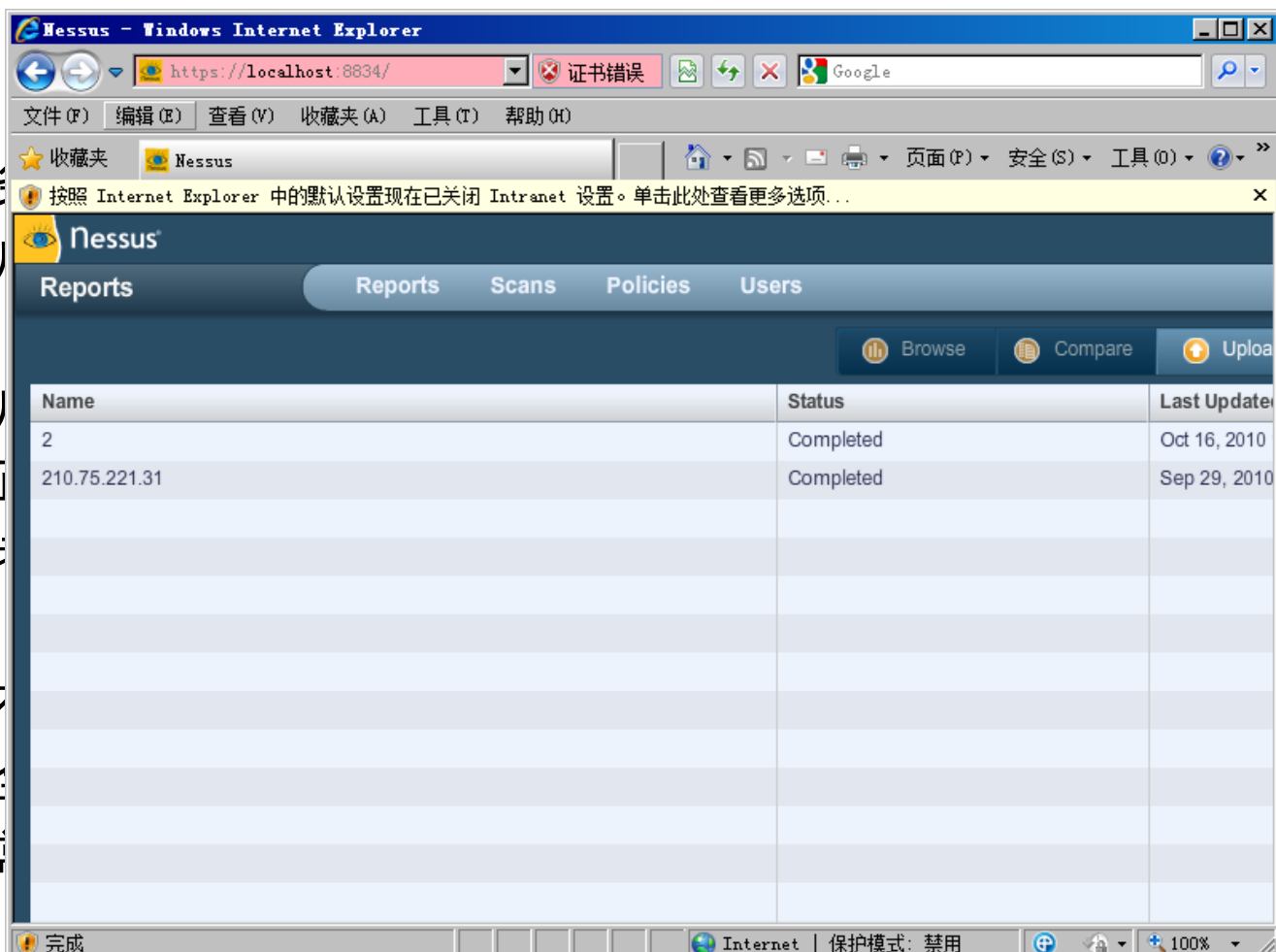
- 服务器
- 客户端

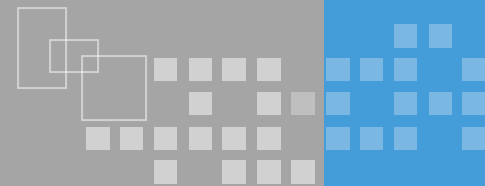
### ■ 运作

- 客户端
- 真实环境
- 两种模式

### ■ 优势:

- 具有
- 完全
- 非常



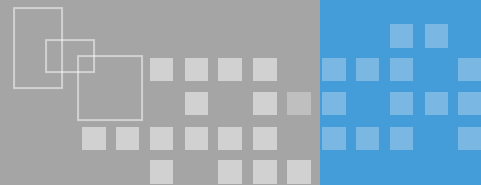


## ❖ 漏洞信息查询

- 漏洞库
- 论坛
- QQ群
- 邮件列表

## ❖ 攻击工具收集

- 黑客网站



## ❖ 公开信息收集防御

- 信息展示最小化原则，不必要的信息不要发布

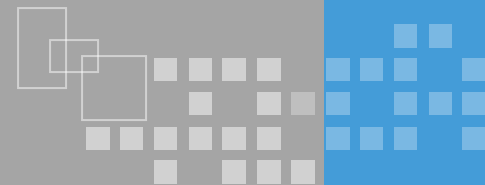
## ❖ 网络信息收集防御

- 阻止ICMP
- 网络安全设备（IDS、防火墙等）

## ❖ 系统及应用信息收集防御

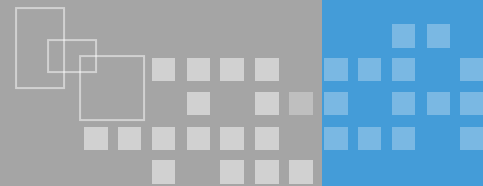
- 减少攻击面
- 修改旗标





## ❖ 知识子域：常见攻击与防范

- 理解默认口令攻击、字典攻击及暴力攻击的原理与防范措施
- 理解社会工程学攻击的方法与防范措施
- 理解IP欺骗、ARP欺骗和DNS欺骗的原理与防范措施
- 理解SYN Flood、UDP Flood、Teardrop攻击等典型DOS/DDOS的原理与防范措施
- 理解缓冲区溢出攻击的原理与防范措施
- 理解SQL注入攻击的原理与防范措施
- 理解跨站脚本攻击的原理与防范措施



## ❖ 密码破解方法

- 暴力猜解

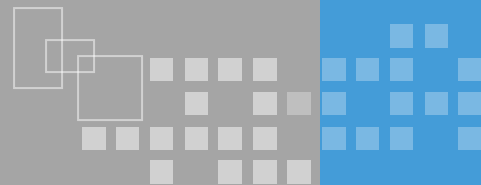
## ❖ 密码破解工具

- 密码暴力破解工具
- 密码字典生成工具

## ❖ 密码破解防御

- 密码生成技巧
- 密码管理策略





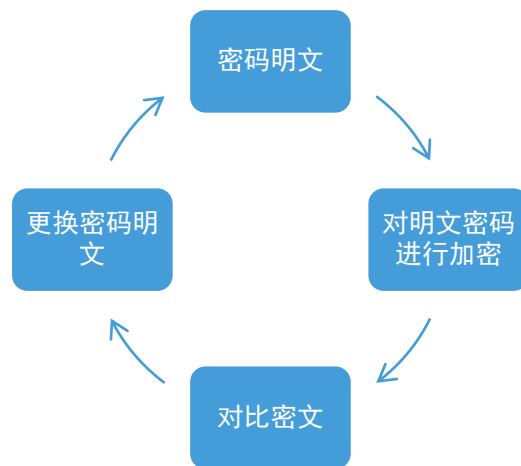
## ❖ 已知密码的散列算法及散列值的破解方法

### ■ Linux密码散列值

#root:\$1\$acQMceF9:13402:0:99999:7:::

### ■ Windows密码散列值 (LM-Hash)

Administrator:500:C8825DB10F2590EAAAD3B435B51404EE  
:683020925C5D8569C23AA724774CE6CC:::





# 暴力猜解工具

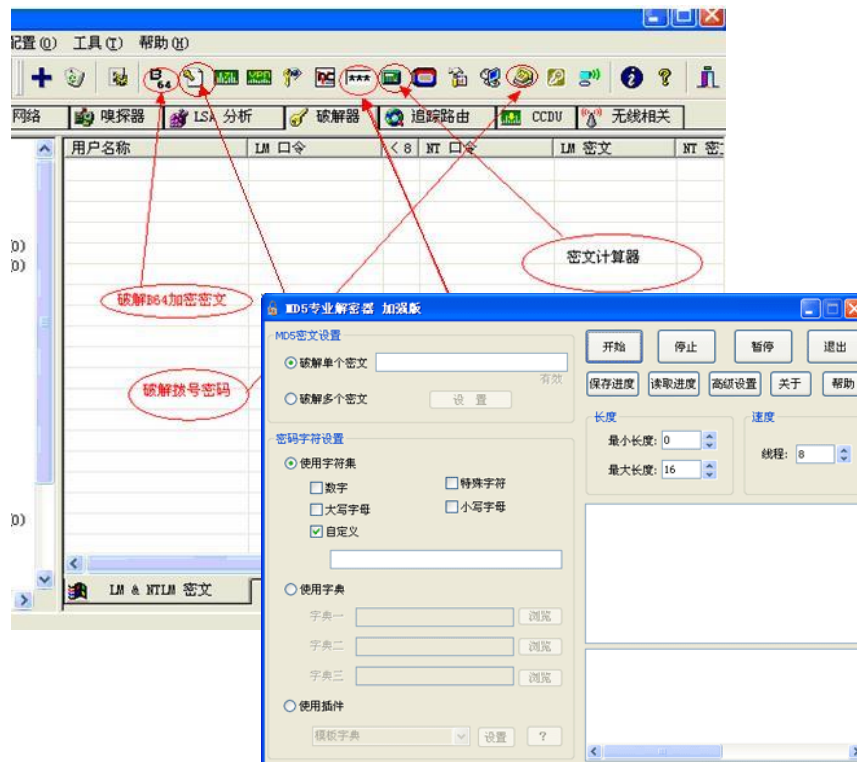
## ❖ 获取散列值

- pwdump7.exe
- GetHashes.exe
- SAMInside.exe
- Cain
- .....

## ❖ 破解散列值

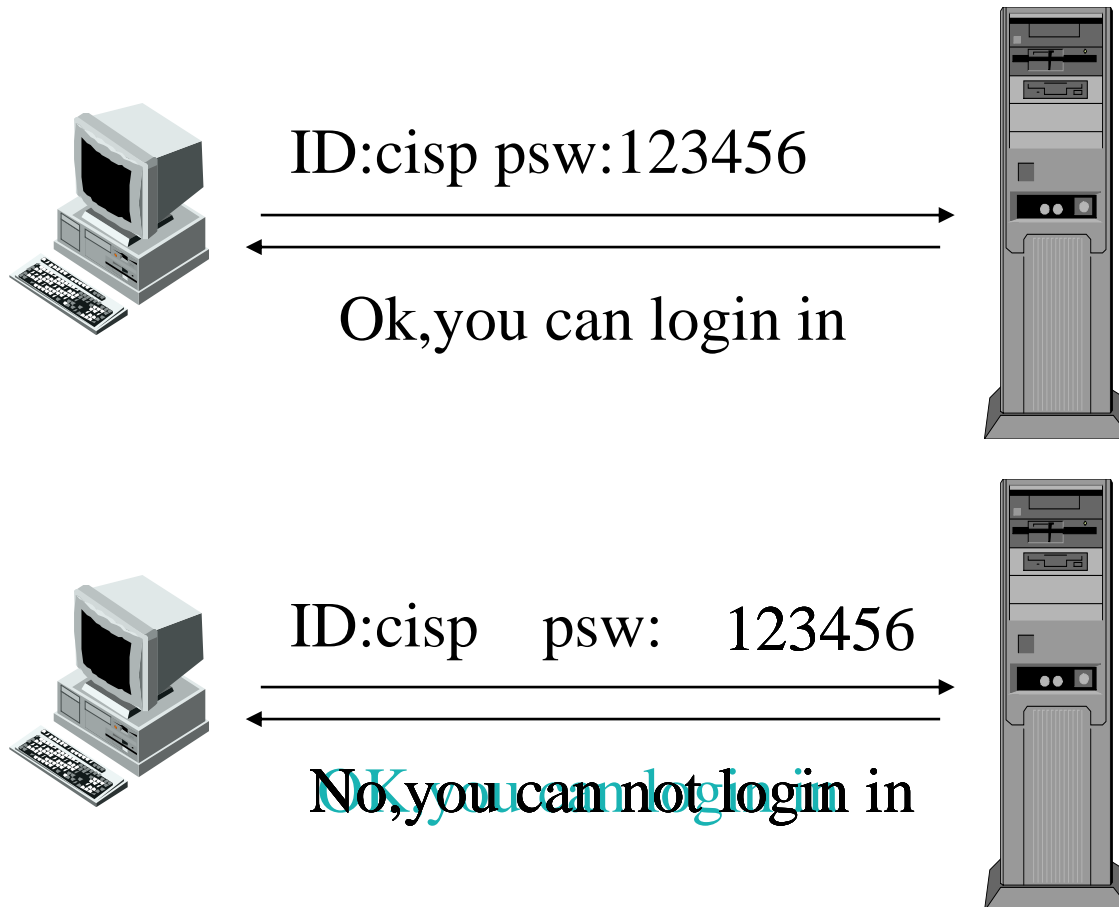
- John the Ripper
- L0Phtcrack

❖ .....





# 暴力猜解方法二





# 密码字典-密码破解关键

## ❖ 字典生成器

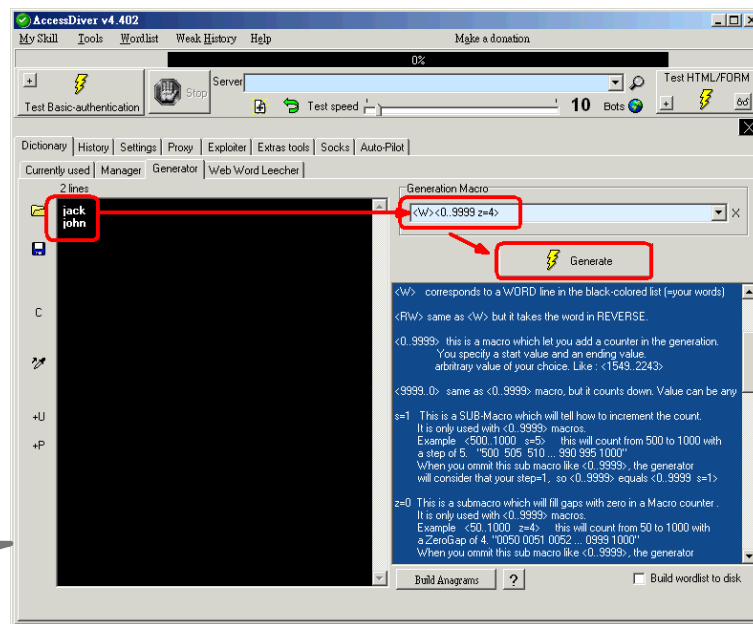
- 根据用户规则快速生成各类密码字典
- 攻击者常用的工具

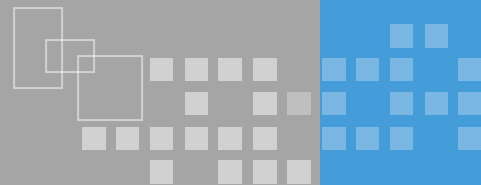
## ❖ 密码字典作用

- 提高密码破解效率
- 密码破解知识的具体体现



密码字典是攻击者破解成功和效率的关键！





## ❖ 系统及应用安全策略对抗密码

- 限制密码尝试次数
- 限制必须提供安全的密码
- 密码有效期等

## ❖ 好的密码特征

- 自己容易记住，别人不好猜

## ❖ 其他密码管理策略

- 密码信封
- A、B角

❖ .....



# 利用人性缺陷-社会工程学攻击

## ❖ 什么是社会工程学攻击

- 利用人性弱点（本能反应、贪婪、易于信任等）进行欺骗获取利益的攻击方法

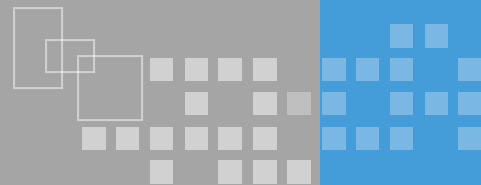
## ❖ 社会工程学的危险

- 永远有效的攻击方法
- 人是最不可控的因素





# 传统社会中的社会工程学



- ❖ 中奖通知
- ❖ 欠费电话
- ❖ 退税短信
- ❖ 好友充值短信
- ❖ .....





# 案例一、凯文·米特尼克最擅长什么

## ❖ 凯文·米特尼克

- 世界著名黑客（世界第一黑客）
- 1995年16岁时被捕入狱，2000年保释
- 记者采访：你最擅长的技术是什么
- 回答：社会工程学，技术会过时，只有社会工程学永远不会

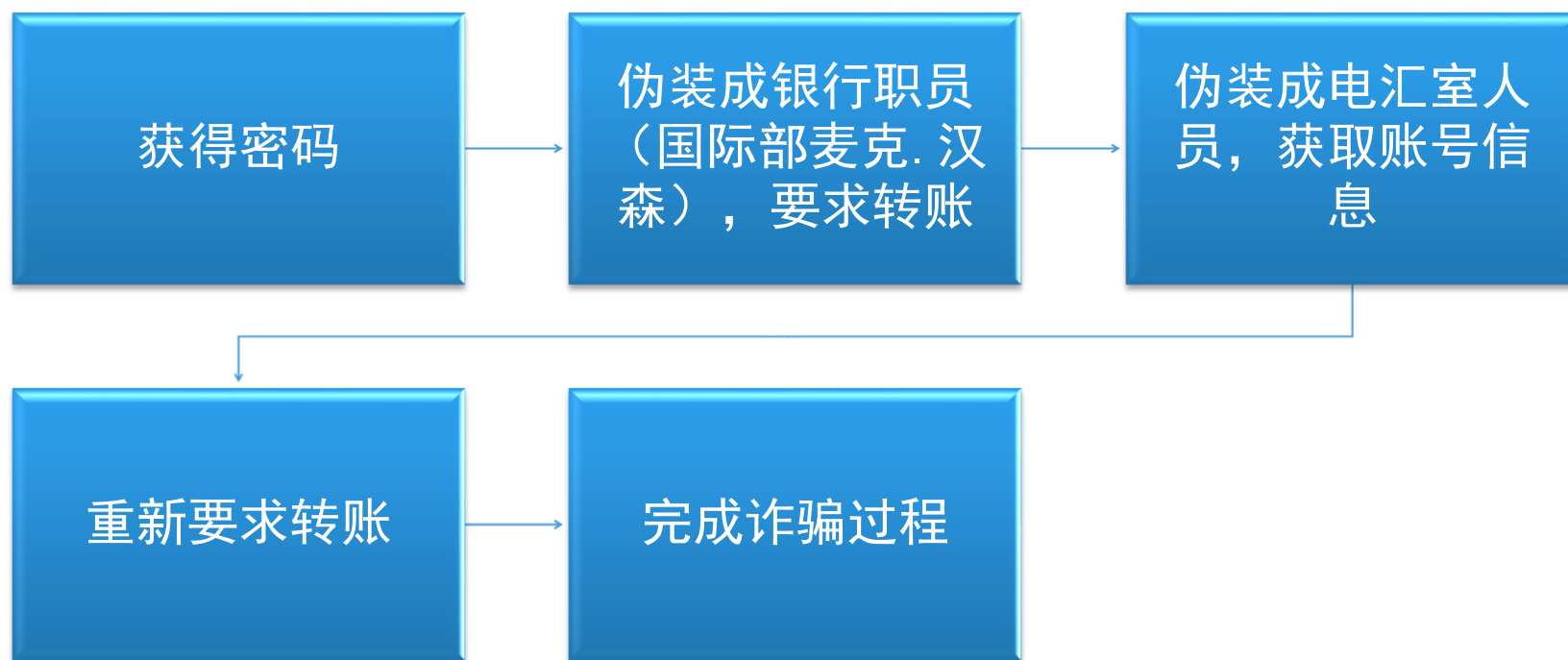


凯文米特尼克所  
著《欺骗的艺术》





## 案例二：“最大的计算机诈骗”过程





## 案例三：好心网管的失误

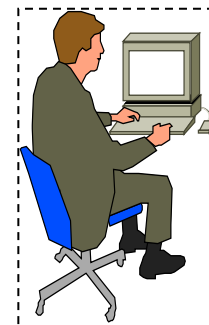
攻击者

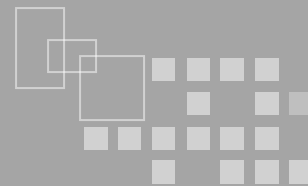


电话网管：你好，我是某某处王强，我的密码忘记了，麻烦帮处理一下

好的，请10分钟后登陆，我帮你把密码重置为123

网站上查询到信息：  
网管联系电话  
某处室人员名称：王强

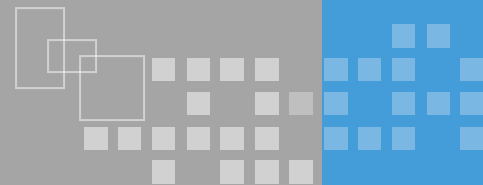




- ❖ 正面攻击-直接索取
- ❖ 建立信任
- ❖ 我来帮助你
- ❖ 你能帮助我吗?
- ❖ 假冒网站和危险附件
- ❖ 利用同情、内疚和胁迫
- ❖ 逆向骗局



# 如何防止社会工程学攻击？



## ❖ 了解攻击者如何利用人的天性并制定针对性培训

- 权威
- 爱好
- 报答
- 守信
- 社会认可
- 短缺

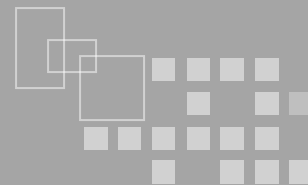
## ❖ 制定针对性安全策略

- 验证身份
- 验证权限
- .....

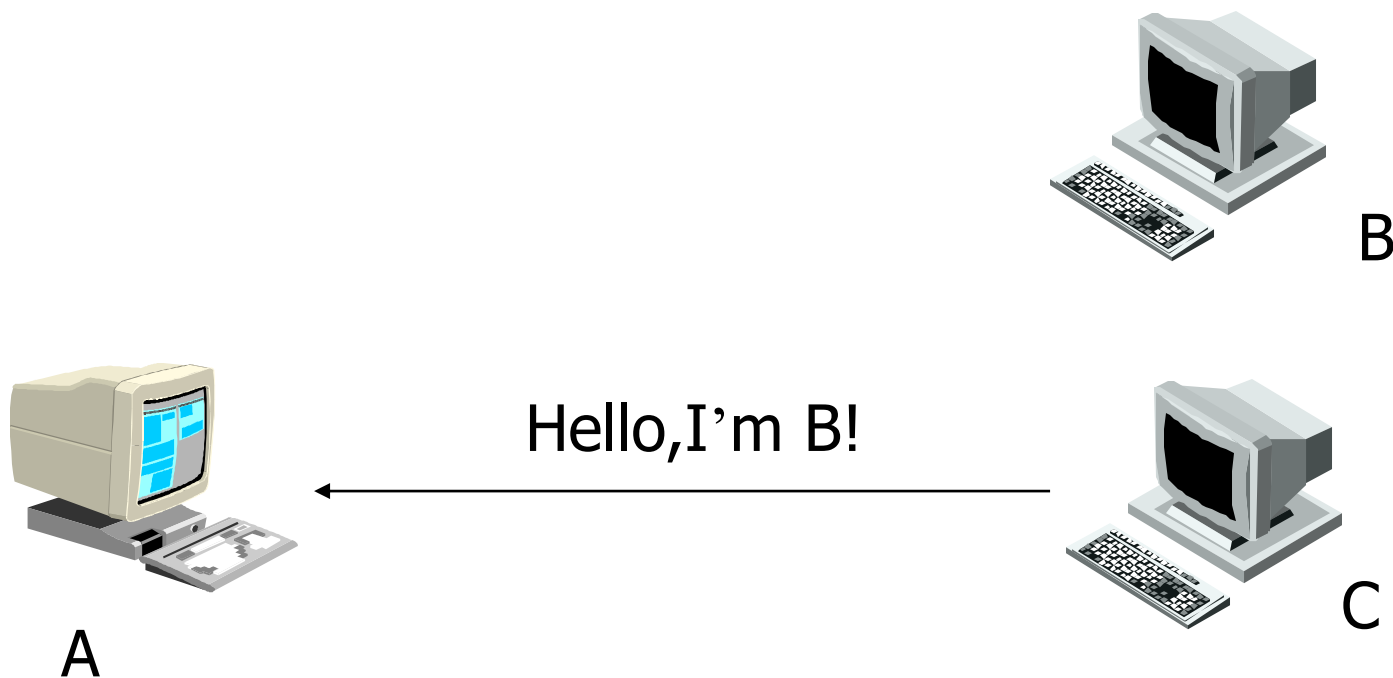




# 利用协议的缺陷-欺骗攻击

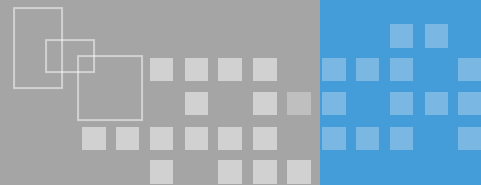


❖ 欺骗攻击（Spoofing）是指通过伪造源于可信任地址的数据包以使一台机器认证另一台机器的复杂技术





# 典型的欺骗攻击

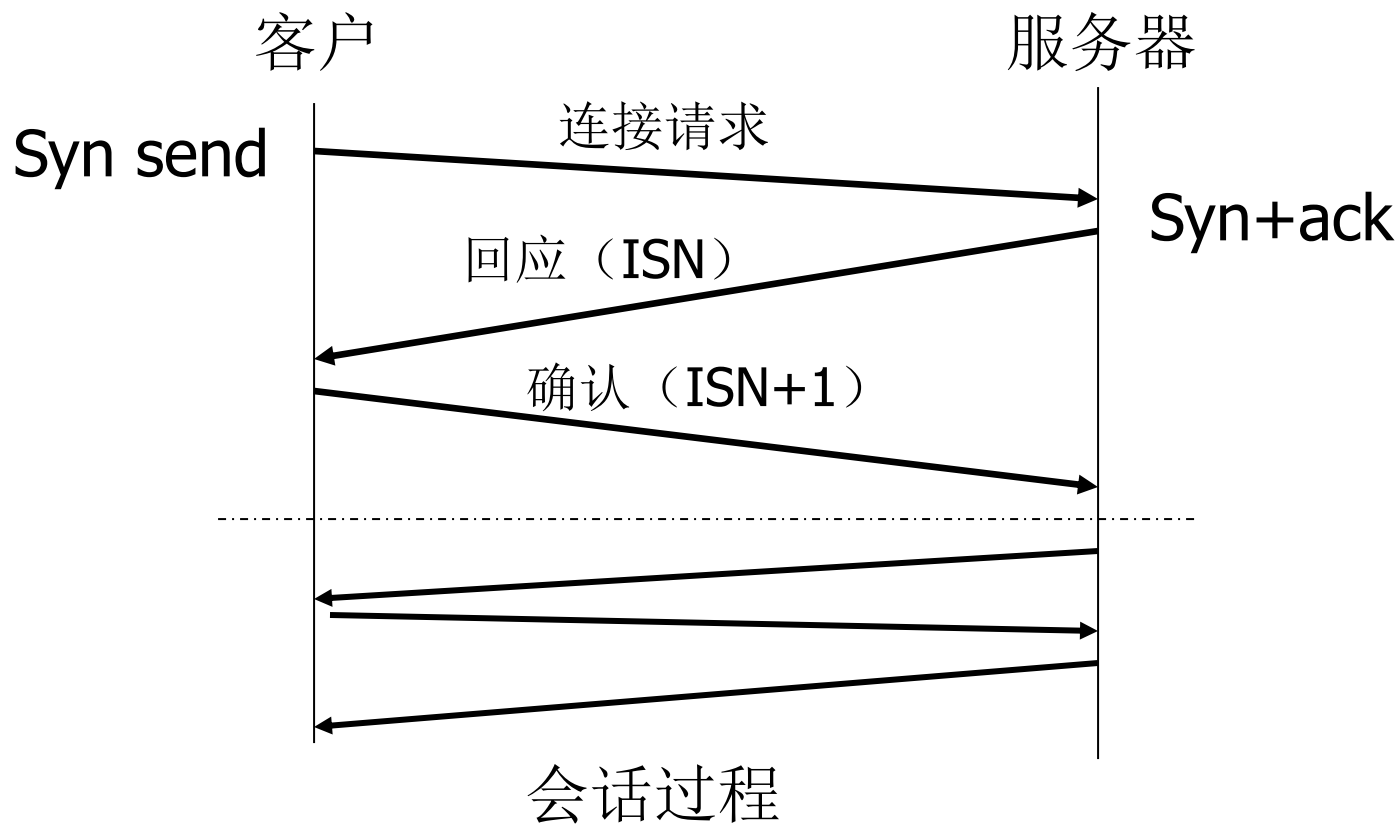
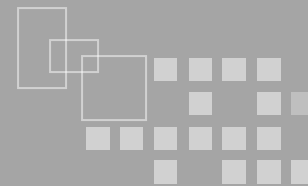


- ❖ IP欺骗 (IP Spoofing)
- ❖ DNS欺骗 (DNS Spoofing)
- ❖ ARP欺骗 (ARP Spoofing)
- ❖ .....

电子欺骗是一类  
攻击方式的统称！

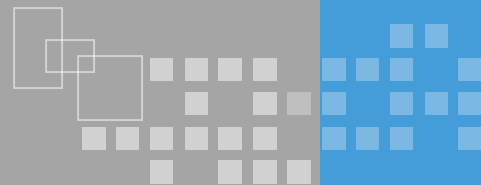


# IP欺骗基础知识-三次握手





# IP欺骗实现步骤



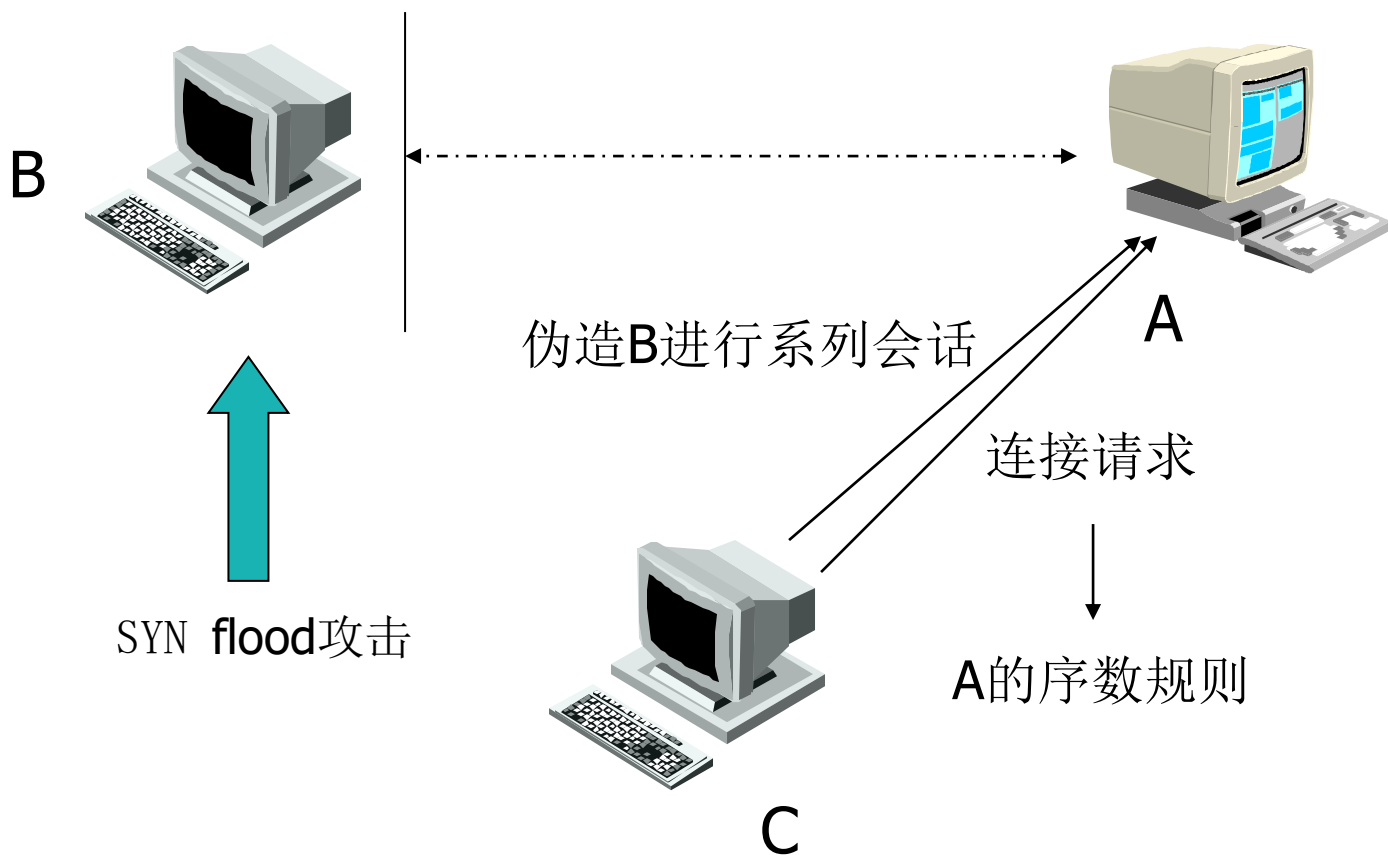
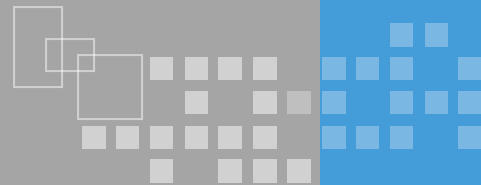
IP欺骗攻击方法中包括了一系列攻击步骤





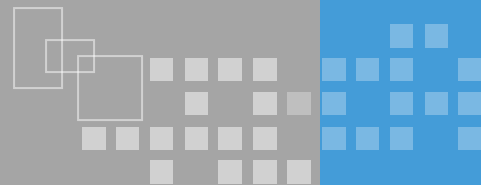


# IP欺骗实例讲解

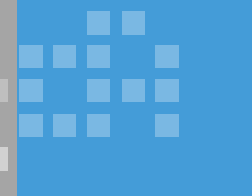
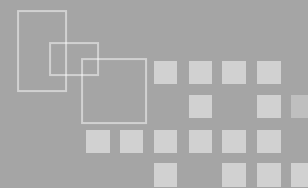




# IP欺骗的防范



- ❖ 严格设置路由策略：拒绝来自网上，且声明源于本地地址的包
- ❖ 使用最新的系统和软件，避免会话序号被猜出
- ❖ 使用抗IP欺骗功能的产品
- ❖ 严密监视网络，对攻击进行报警



## ❖ ARP协议（地址解析协议）

- ARP用于将IP地址解析MAC地址的协议
- ARP协议特点：无状态，无需请求可以应答
- ARP实现：ARP缓存

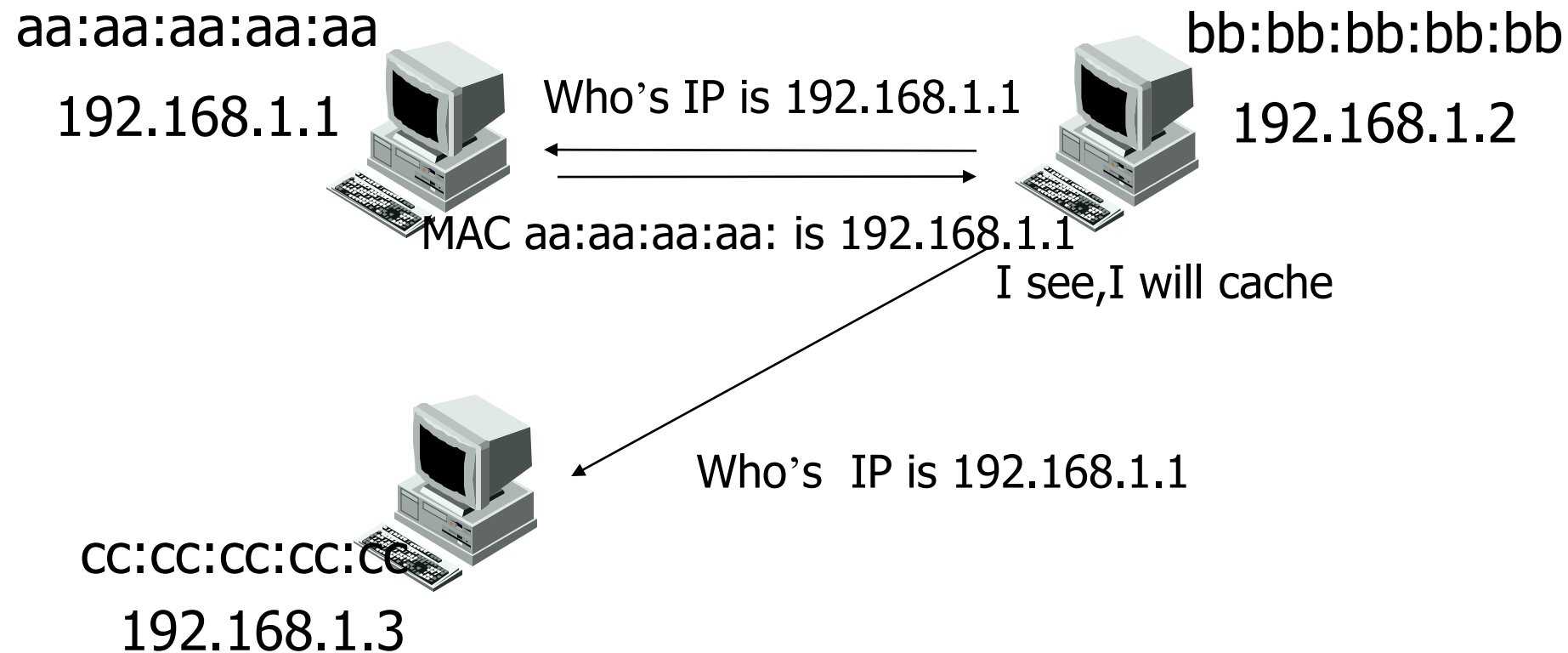
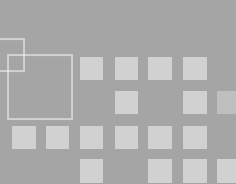
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\scn>arp -a

接口: 192.168.0.30 --- 0xb
Internet 地址      物理地址      类型
192.168.0.1        00-25-9e-14-dc-4b 动态
192.168.0.255      ff-ff-ff-ff-ff-ff 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.252        01-00-5e-00-00-fc 静态
239.255.255.250    01-00-5e-7f-ff-fa 静态
```

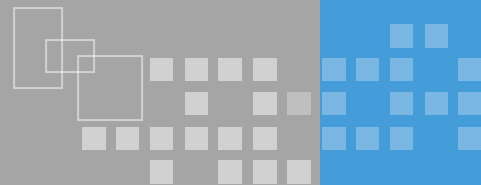


# ARP欺骗基础-Arp协议工作过程





# ARP欺骗实现



Internet地址

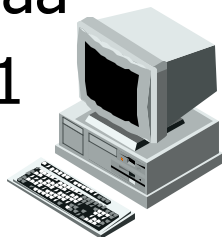
物理地址

192.168.1.1

cc:cc:cc:cc:cc

aa:aa:aa:aa:aa

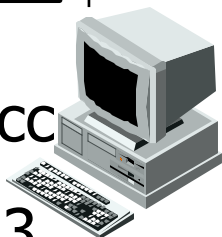
192.168.1.1



AA:AA:AA:AA:AA
192.168.1.1
Hello

cc:cc:cc:cc:cc

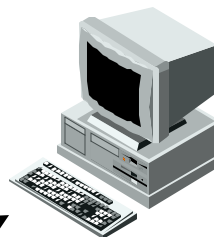
192.168.1.3



CC:CC:CC:CC:CC
192.168.1.1
Hello

bb:bb:bb:bb:bb

192.168.1.2

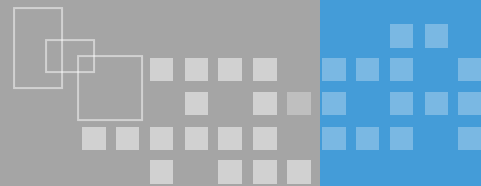


I see,I will cache

MAC cc:cc:cc:cc:cc is 192.168.1.1



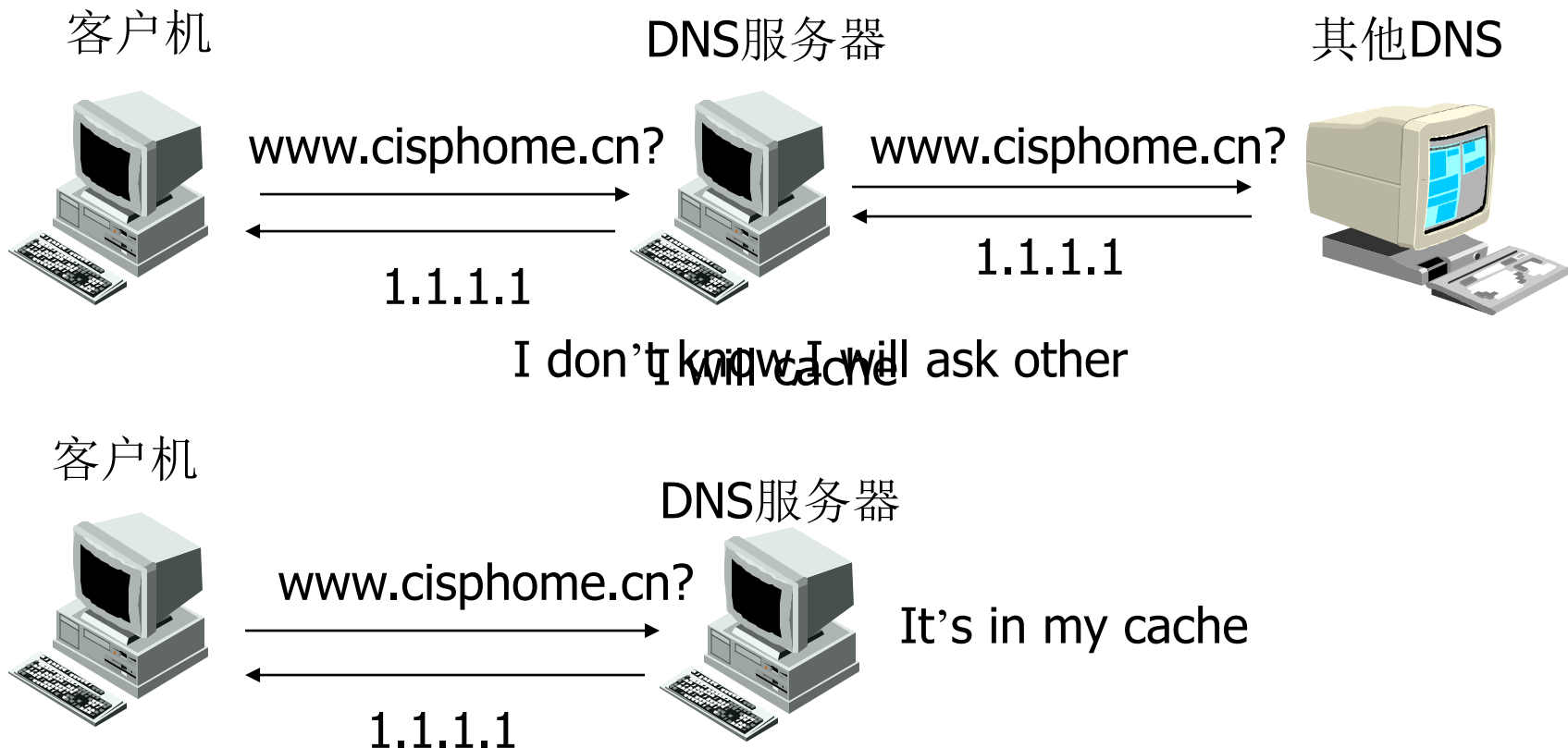
# ARP欺骗的防范



- ❖ 使用静态ARP缓存
- ❖ 使用三层交换设备
- ❖ IP 与MAC地址绑定
- ❖ ARP防御工具

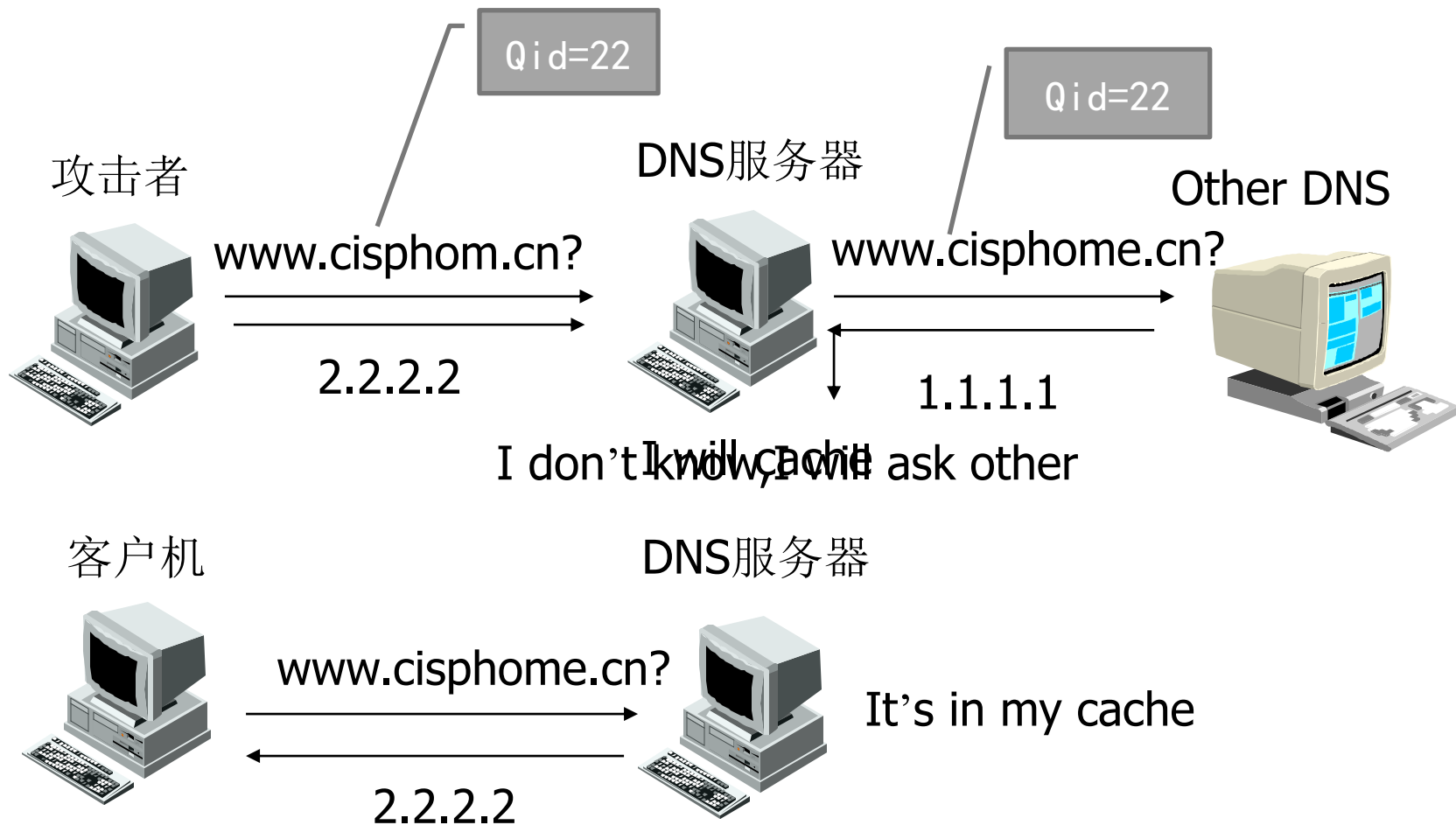
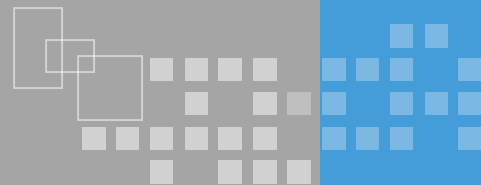


# DNS欺骗基础-DNS协议工作过程

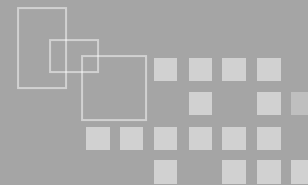




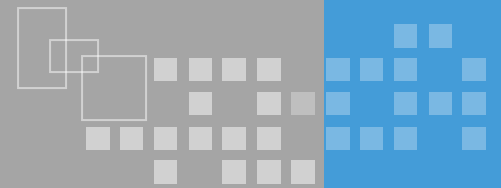
# DNS欺骗实现







- ❖ 安装最新版本的DNS软件
- ❖ 安全设置对抗DNS欺骗
  - 关闭DNS服务递归功能
  - 限制域名服务器作出响应的地址
  - 限制域名服务器作出响应的递归请求地址
  - 限制发出请求的地址

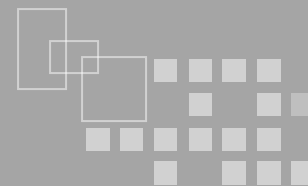


## ❖ TCP会话劫持

## ❖ 路由欺骗

- ICMP重定向报文
- RIP路由欺骗
- 源径路由欺骗





## ❖ 什么是拒绝服务

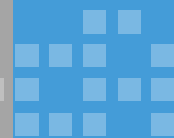
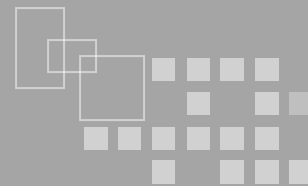
- 拒绝服务式攻击 (Denial of Service), 顾名思义就是让被攻击的系统无法正常进行服务的攻击方式。

## ❖ 拒绝服务攻击方式

- 利用大量数据挤占网络带宽
- 利用大量请求消耗系统性能
- 利用协议实现缺陷
- 利用系统处理方式缺陷



# 典型的拒绝服务攻击方式



❖ Ping of death

❖ SYN Flood

❖ UDP Flood

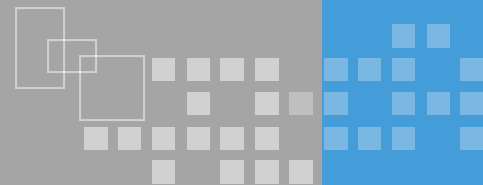
❖ Teardrop

❖ Land

❖ Smurf

❖ .....

拒绝服务是一类  
攻击方式的统称！



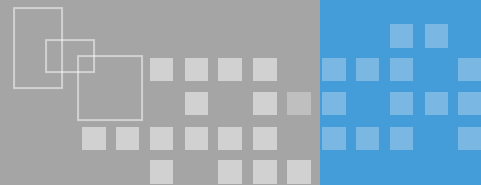
## ❖ 原理

- Ping使用ICMP协议数据包最大为65535
- 构造错误的ICMP数据报文（错误的偏移值和分片大小），在重组时会产生大于65535的数据包，导致填入堆栈时产生缓冲区溢出

错误的ICMP重组数据报文

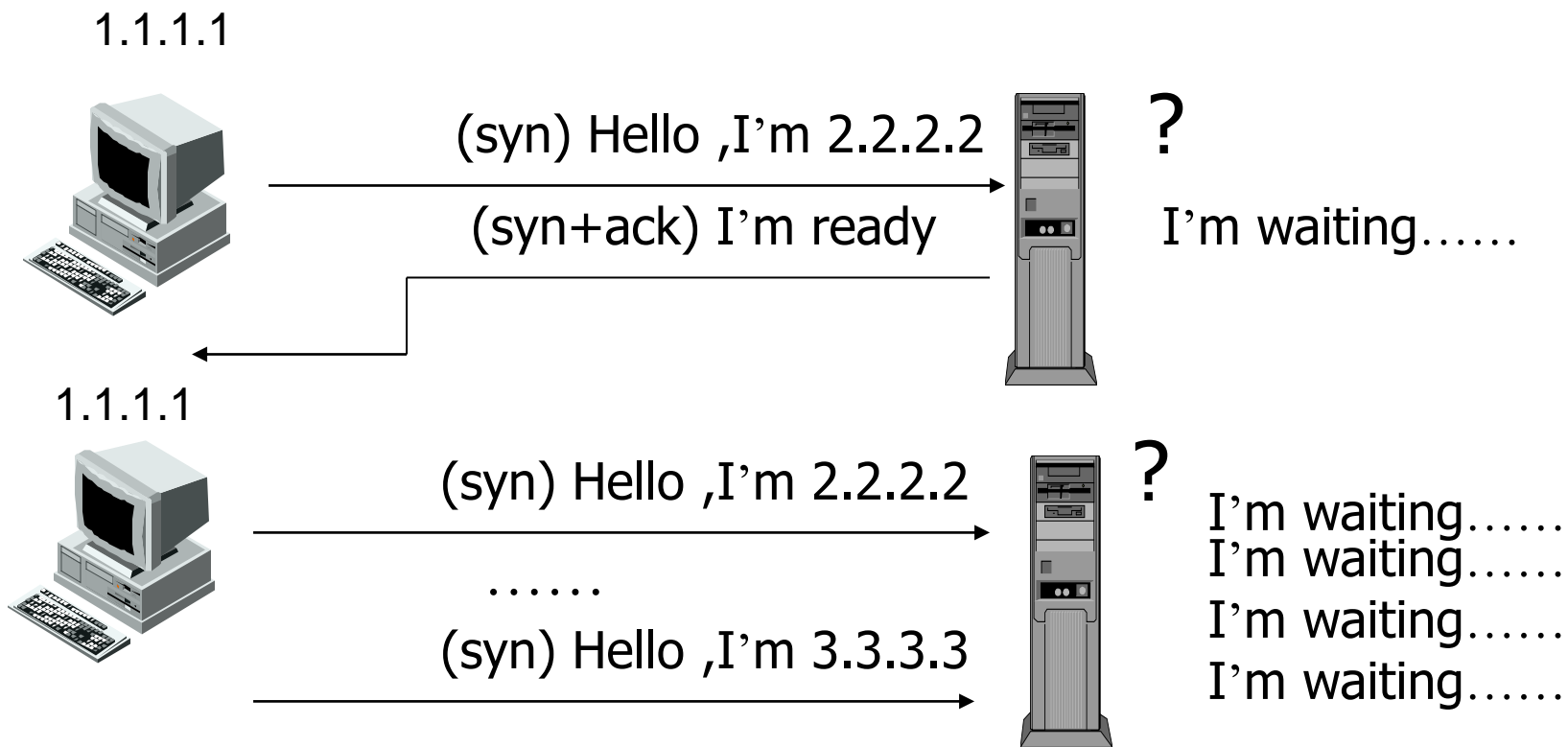
ICMP协议堆栈

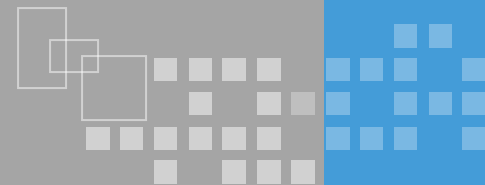
其他内存空间



## ❖ 原理

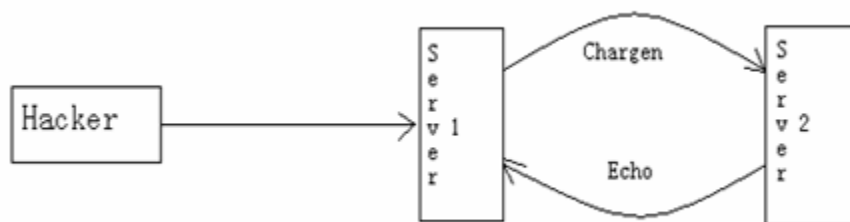
- 伪造虚假地址连接请求，消耗主机连接数





## ❖ 原理

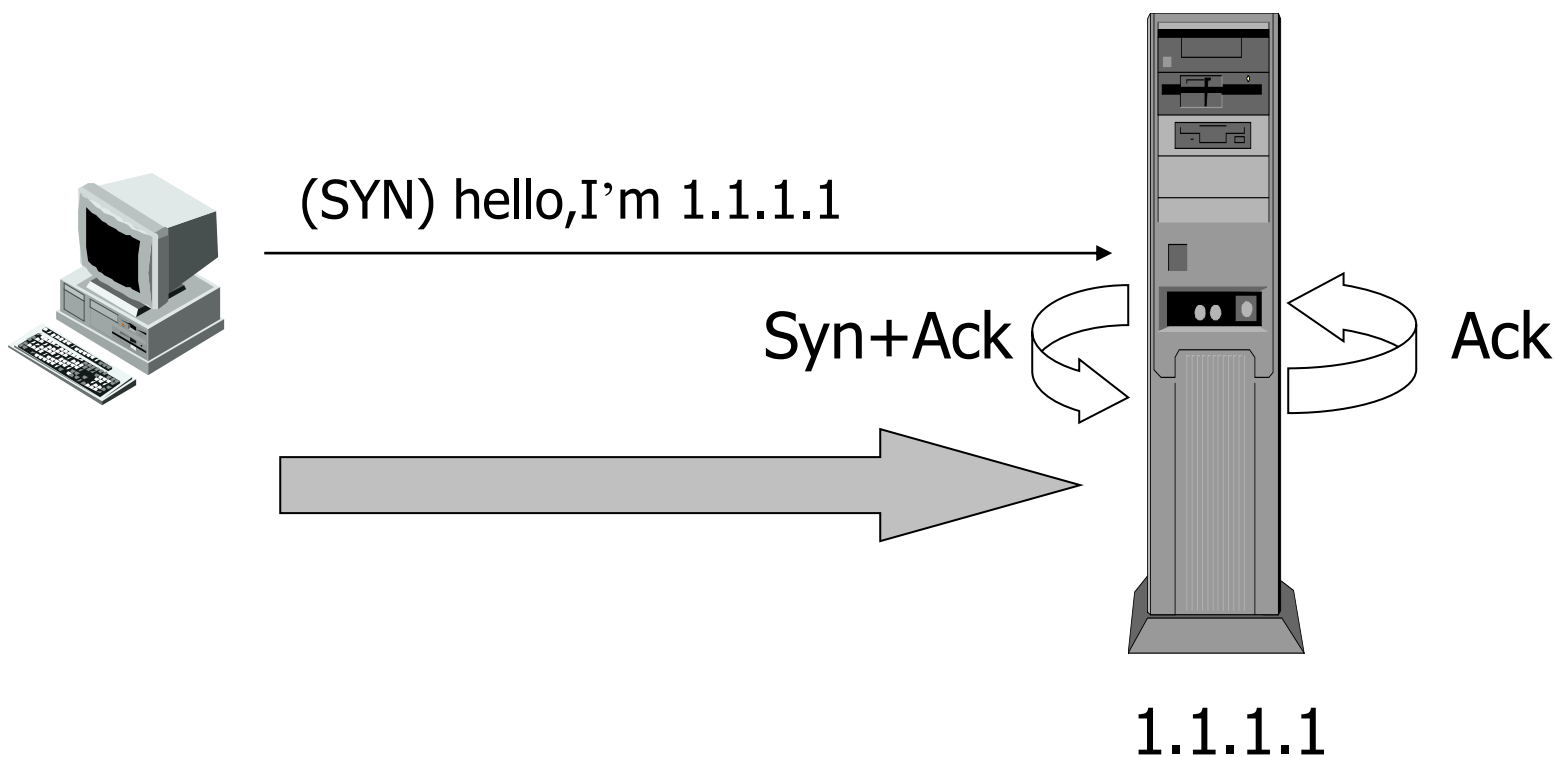
- 利用UDP协议实现简单、高效，形成流量冲击
- 实现方式
  - 大量UDP小包冲击应用服务器（DNS、Radius认证等）
  - 利用系统服务形成流量（Echo chargen）
  - 利用正常UDP服务发送大流量形成网络拥塞





## ❖ 原理

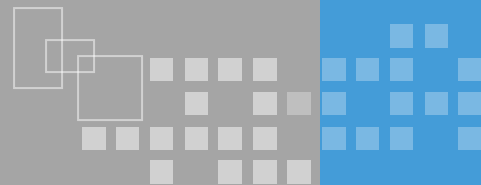
- 类似SYN flood，伪造受害主机源地址发送连接请求，使受害主机形成自身连接，消耗连接数





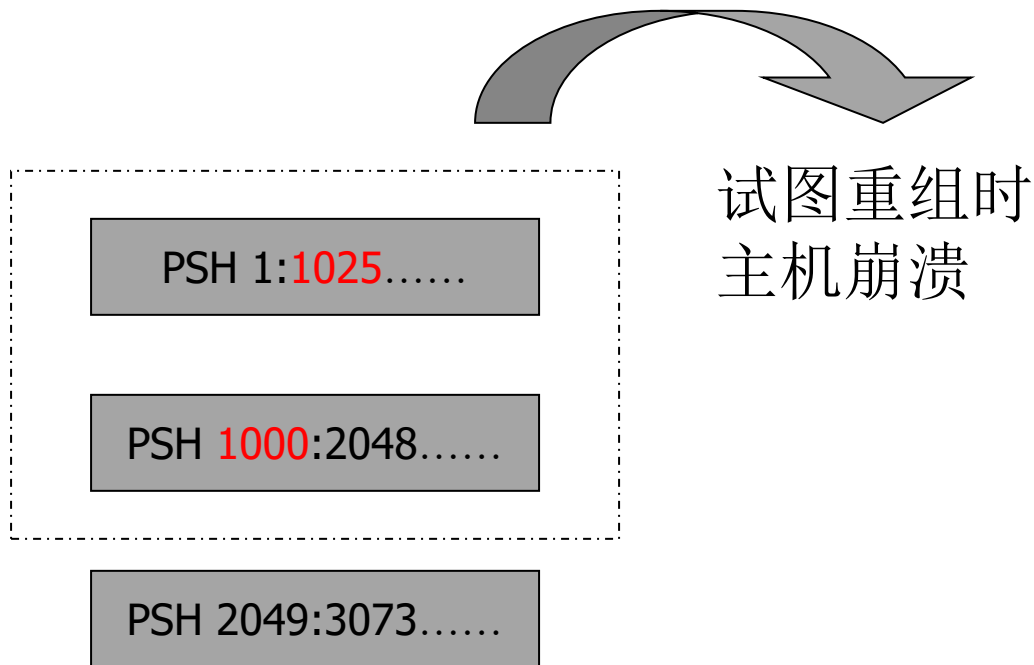
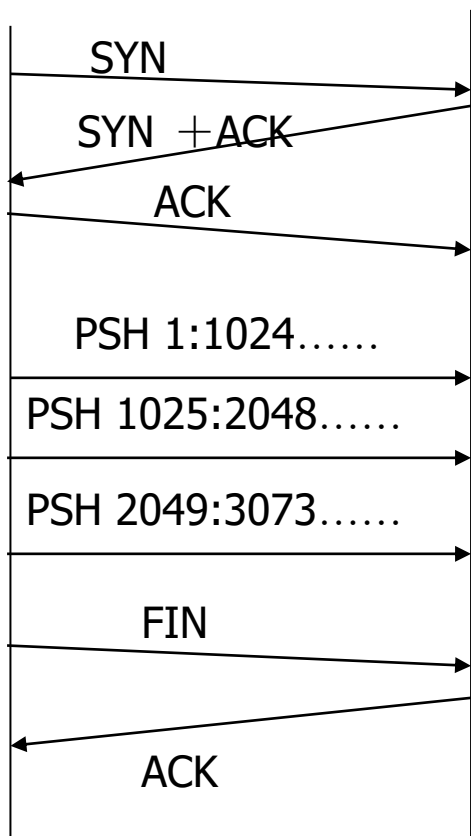


# TearDrop (分片攻击)



## ❖ 原理

- 构造错误的分片信息，系统重组分片数据时内存计算错误，导致协议栈崩溃

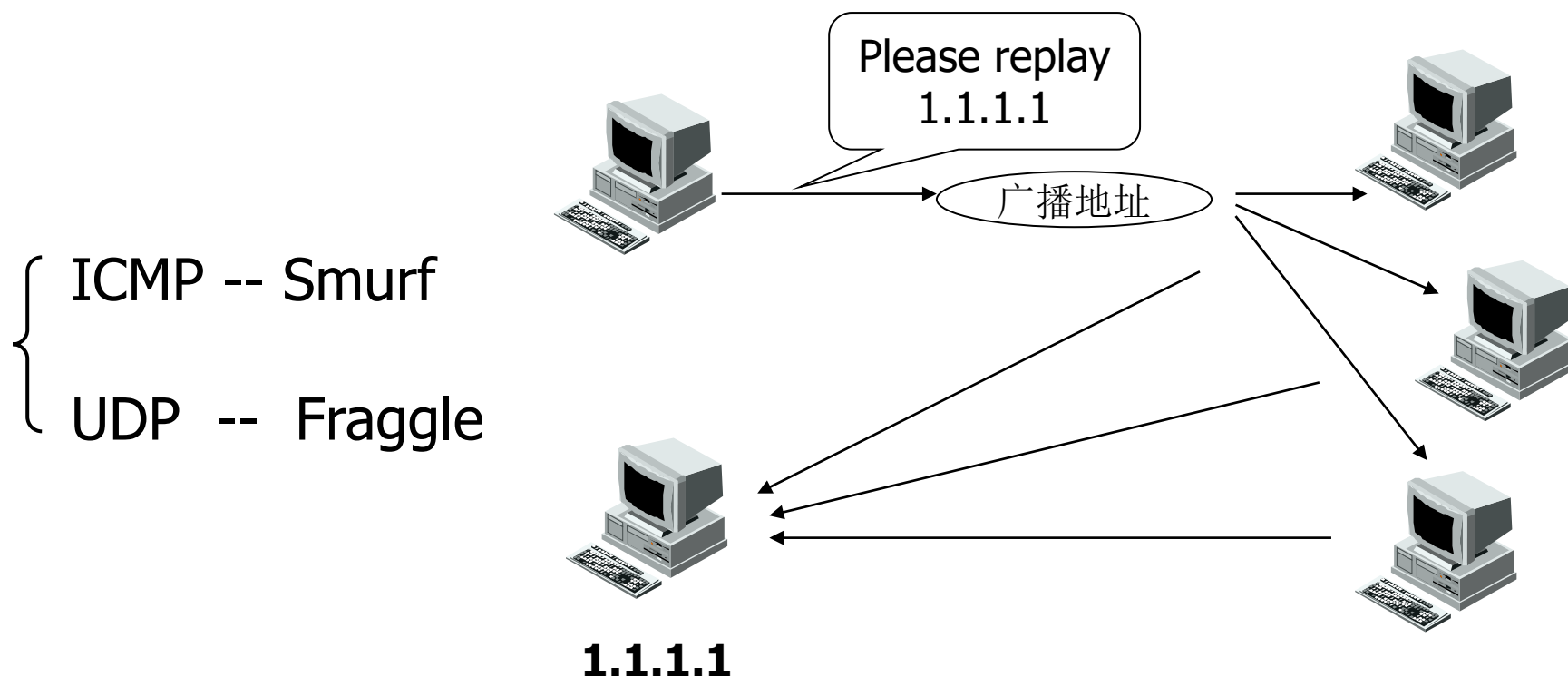




# Smurf&Fraggle攻击

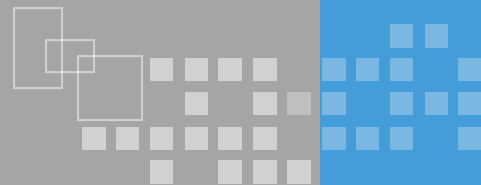
## ❖ 原理

- 伪造受害者地址向广播地址发送应答请求，要求其他机器响应，形成流量攻击





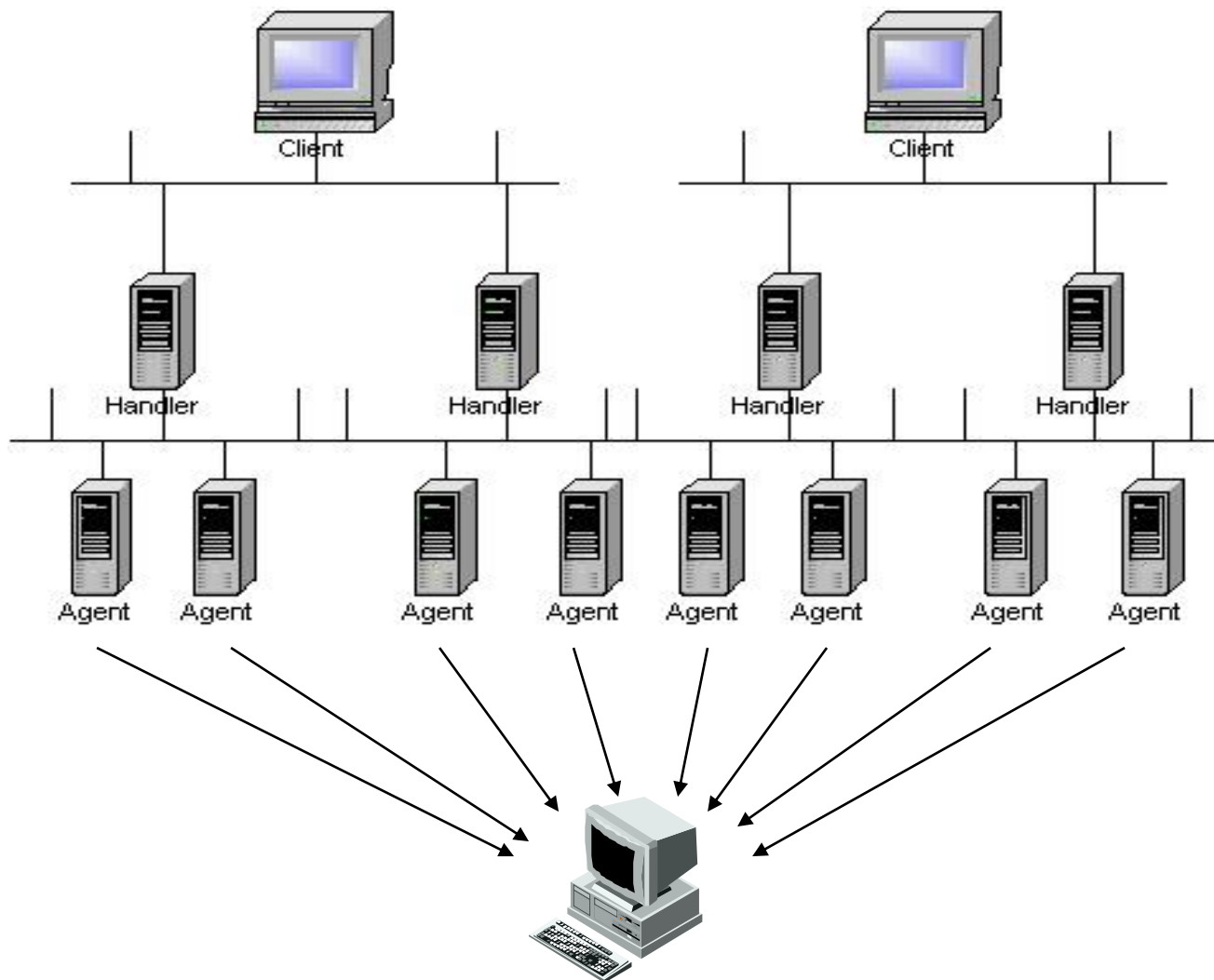
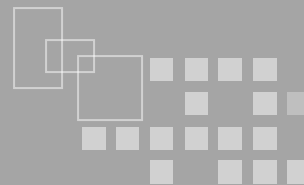
# 拒绝服务攻击的危害



- ❖ 消耗带宽
- ❖ 瘫痪服务器
  - DNS
  - 网页
  - 电子邮件
- ❖ 阻塞网络
  - 路由器
  - 交换器

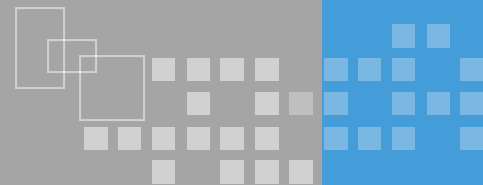


# DDoS攻击原理



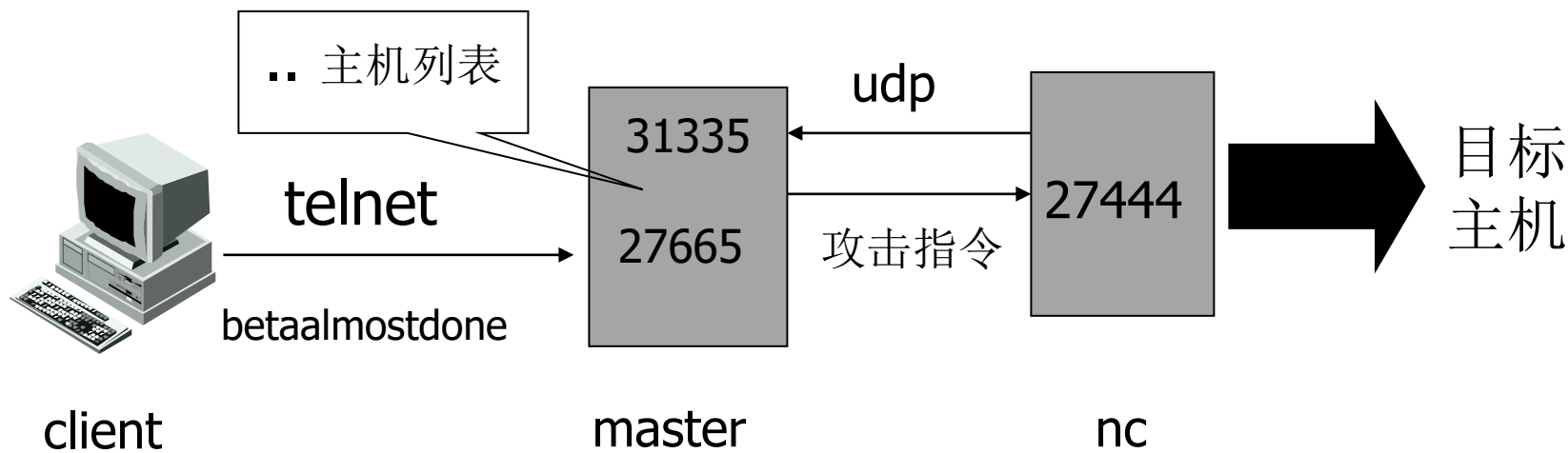


# 典型的DDoS攻击工具



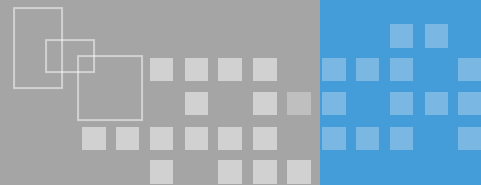
❖ TFN2K

❖ Trinoo





# 拒绝服务攻击的防范



## ❖ 增强自身强壮性

- 风险评估
- 补丁
- 安全加固
- 资源控制

## ❖ 加强防御

- 安全设备（防火墙、抗DoS设备）
- 网络带宽

## ❖ 协调机制

- 运营商、公安部门、专家团队等



## ❖ 缓冲区溢出原理

- 缓冲区溢出攻击利用编写不够严谨的程序，通过向程序的缓冲区写入超过预定长度的数据，造成缓存的溢出，从而破坏程序的堆栈，导致程序执行流程的改变。

## ❖ 基础知识

- 堆栈
- 寄存器
- 指针



# 缓冲区溢出基础-堆栈、指针、寄存器

## ❖ 堆栈概念

- 一段连续分配的内存空间

## ❖ 堆栈特点

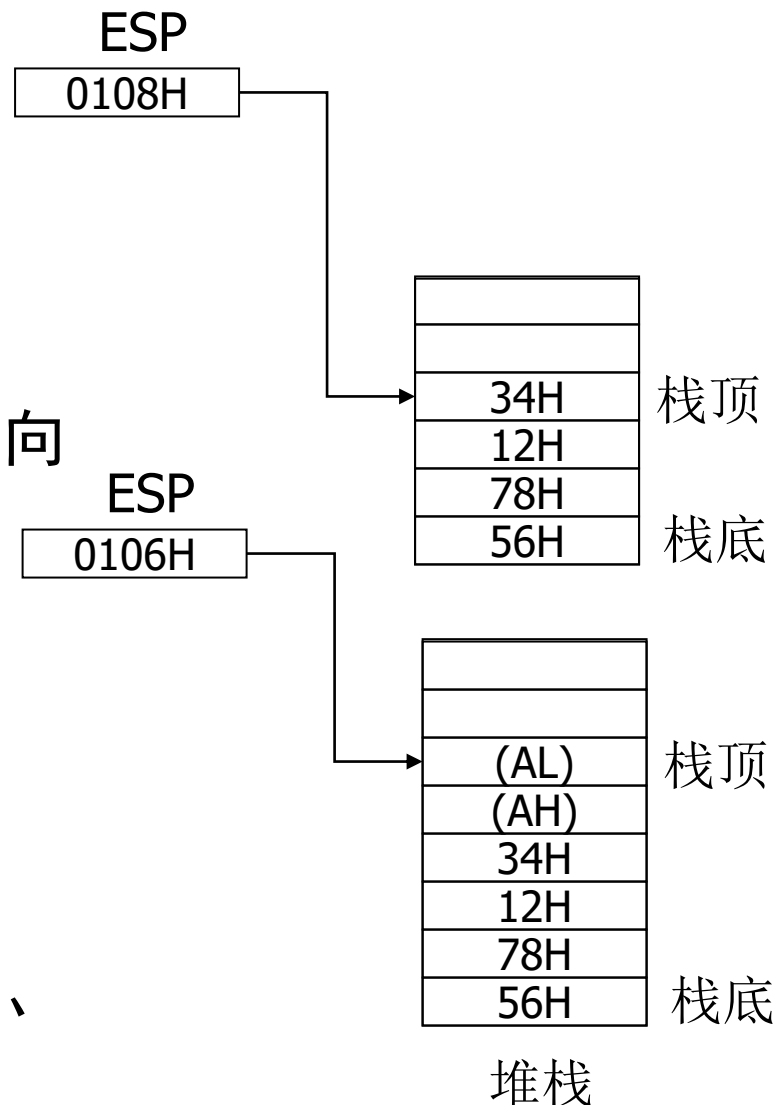
- 后进先出
- 堆栈生长方向与内存地址方向相反

## ❖ 指针

- 指针是指向内存单元的地址

## ■ 寄存器

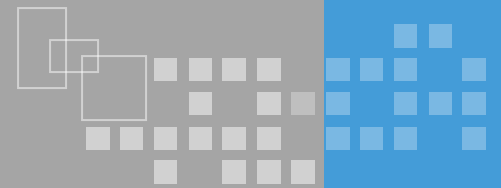
- 暂存指令、数据和位址
- ESP（栈顶）、EBP（栈底）、EIP（返回地址）







# 简单示例



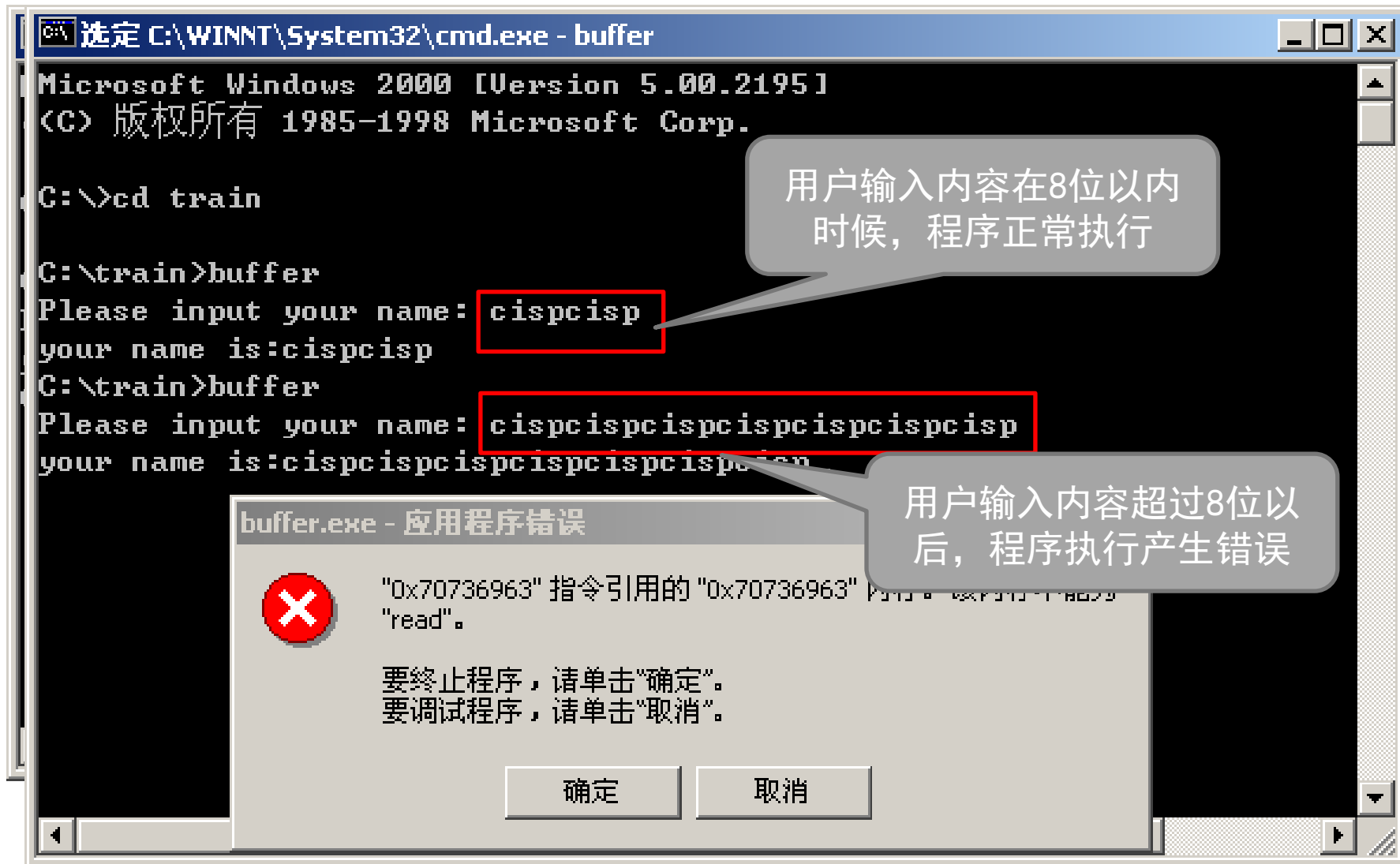
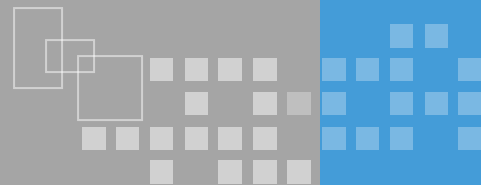
程序作用：  
将用户输入的内容  
打印在屏幕上

Buffer.c

```
#include <stdio.h>
int main ( )
{
    char name[8];
    printf("Please input your name: ");
    gets(name);
    printf("you name is: %s!", name);
    return 0;
}
```

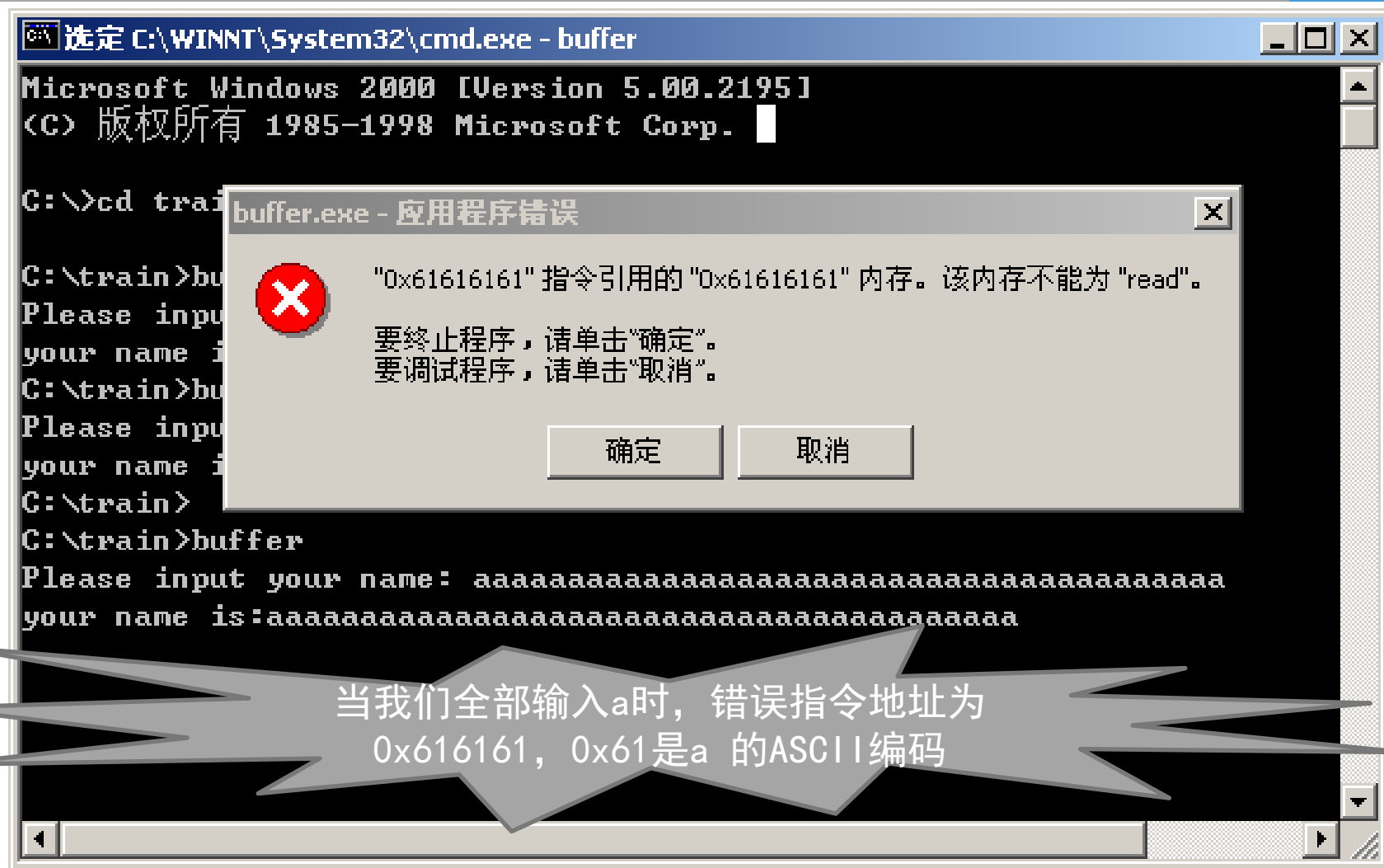
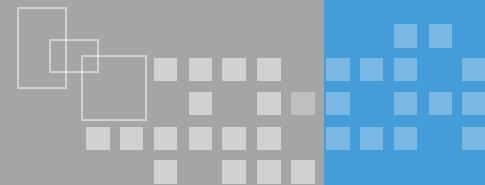


# 简单示例



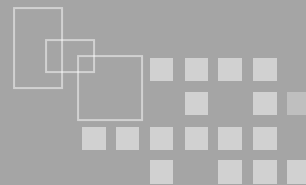


# 简单示例





# 堆栈情况



内存底部

内存顶部

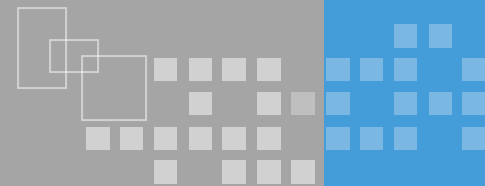
name	XXX	EIP	XXX
[cispcisp]	[     ]	[     ]	[     ]

name	XXX	EIP	XXX
[aaaaaaaa]	[aaaa]	[aaaa]	[aaaa]

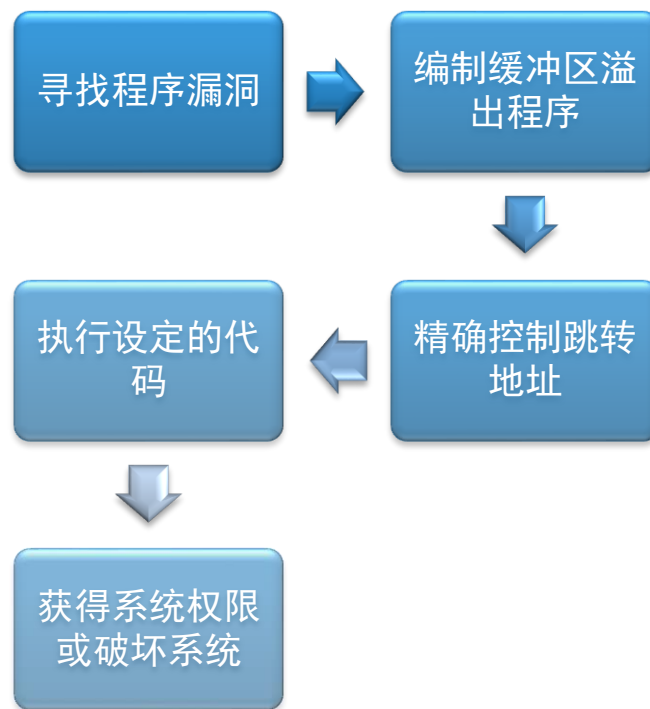
由于输入的name超过了定义变量的长度（8位），堆栈中预计的位置无法容纳，只好向内存顶部继续写‘a’，由于堆栈的生长方向与内存的生长方向相反，用户输入的‘a’覆盖了堆栈底部EBP和ret。程序在返回时，将EBP中的‘aaaa’的ASCII码：0x61616161作为返回地址，试图执行0x61616161处指令，导致错误，形成一次堆栈溢出



# 缓冲区溢出危害

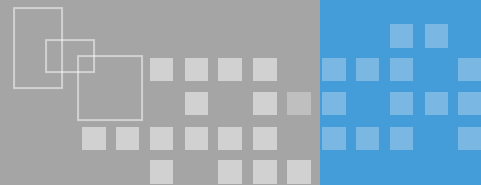


危害：如果可精确控制内存跳转地址，就可以执行指定代码，获得权限或破坏系统





# 缓冲区溢出的防范



## ❖ 用户

- 补丁
- 防火墙

## ❖ 开发人员

- 编写安全代码，对输入数据进行验证
- 使用相对安全的函数

## ❖ 系统

- 缓冲区不可执行技术，使被攻击程序的数据段地址空间不可执行，从而使攻击者不可能执行输入缓冲区的代码
- 虚拟化技术

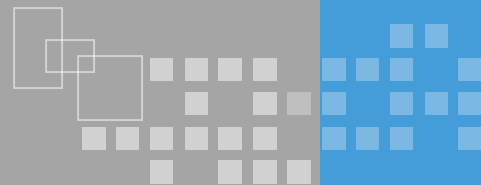


## ❖ 脚本安全基础

- WEB应用开发脚本: ASP、PHP、JSP等
- 脚本的优势:
  - 交互性:
  - 自动更新:
  - 因时因人而变:

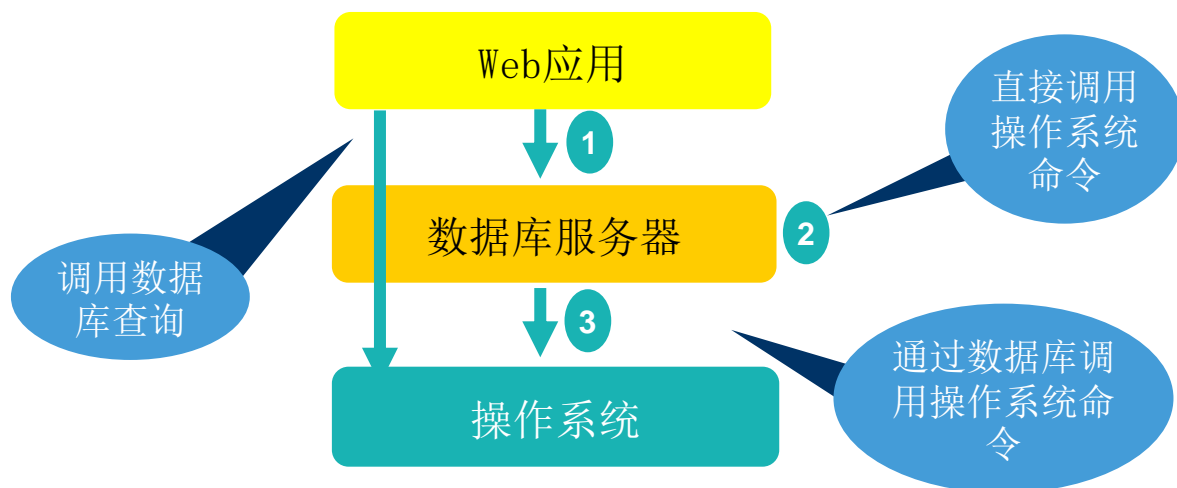
## ❖ 脚本安全风险

- 注入攻击
- 跨站脚本
- .....



## ❖ SQL注入攻击原理

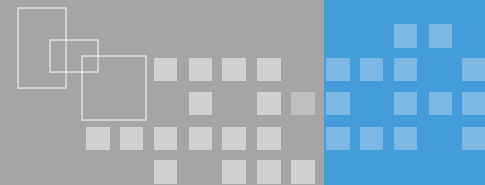
- SQL注入（SQL Injection）：程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据或进行数据库操作







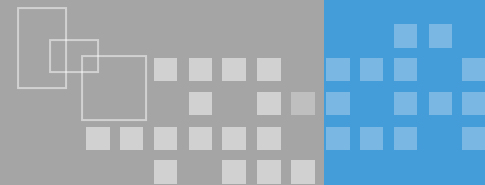
# SQL注入基础知识



- ❖ SQL (Structured Query Language) : 结构化的查询语言，是关系型数据库通讯的标准语言。
- ❖ 查询: `Select statement from table where condition`
- ❖ 删除记录: `delete from table where condition`
- ❖ 更新记录: `update table set field=value where condtion`
- ❖ 添加记录: `insert into table field values(values)`
- ❖ 常用函数
  - `Count()`
  - `Asc( 'nchar' ), unicode( 'nchar' )`
  - `mid(str, n1, n2), substring(str, n1, n2)`



# SQL注入简单示例



用户登陆

用户

密码

**Select \* from table where  
user='admin' and pwd='ABCDEFGH!';**

由于密码的输入方式，使得查询语句  
返回值永远为True，  
因此通过验证

用户登陆

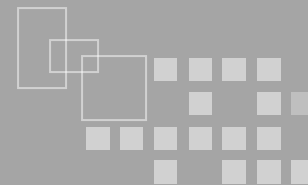
用户

密码

**Select \* from table where  
user='admin' and pwd='123' or '1=1';**



# SQL注入范例-检测



`http://xx.xxx.xx.xx/playnews.asp?id=772' and '1=1`

Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'

[Microsoft][ODBC Microsoft Access Driver] 字符串的语法错误 在查询表达式 'id = 772'' 中。

/displaynews.asp, 行31

说明:

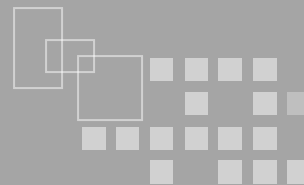
数据库为Access

程序没有对于id进行过滤

数据库表中有个字段名为id



# SQL注入范例一操作数据库



`http://www.test.com/showdetail.asp?id=49' And (update user set passwd='123' where username='admin');--`



`Select * from 表名 where 字段='49' And (update user set passwd='123' where username='admin');`

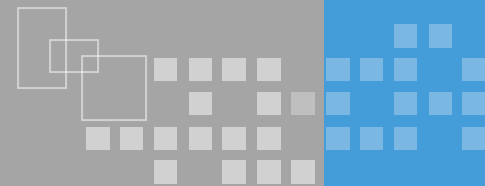


`update user set passwd='123' where username='admin');`

非法的SQL语句被传递到数据库执行！



# SQL注入的危害



## ❖ 数据库信息收集

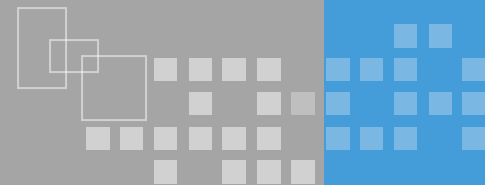
- 数据检索

## ❖ 操作数据库

- 增加数据
- 删除数据
- 更改数据

## ❖ 操作系统

- 借助数据库某些功能（例如：SQLServer的内置存储过程XP\_CMDShell）

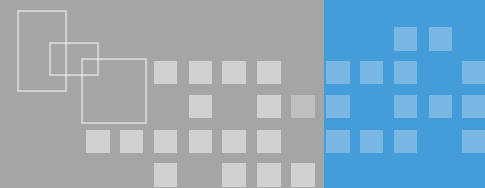


## ❖ 防御的对象：所有外部传入数据

- 用户的输入
  - 提交的URL请求中的参数部分
  - 从cookie中得到的数据
- 其他系统传入的数据

## ❖ 防御的方法

- 白名单：限制传递数据的格式
- 黑名单：过滤
  - 过滤特殊字串：update、insert、delete等
  - 开发时过滤特殊字符：单引号、双引号、斜杠、反斜杠、冒号、空字符等的字符
- 部署防SQL注入系统或脚本



## ❖ 原理

- 远程Web页面的HTML代码中插入的具有恶意目的的数据，用户认为该页面是可信的，当浏览器下载该页面时，嵌入其中的脚本将被解释执行
- 跨站脚本（CSS - Cross Site Scripting）

## ❖ 跨站脚本成因

- CGI程序没有对用户提交的变量中的HTML代码进行过滤或转换。
- 这种攻击利用的是用户和服务端之间的信任关系，以及Web站点没有使用有效的输入输出验证来拒绝嵌入的脚本。



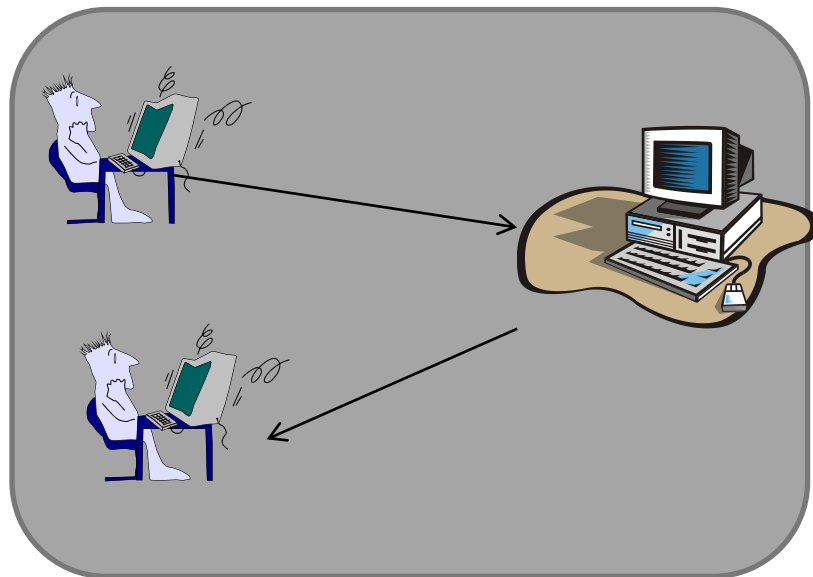
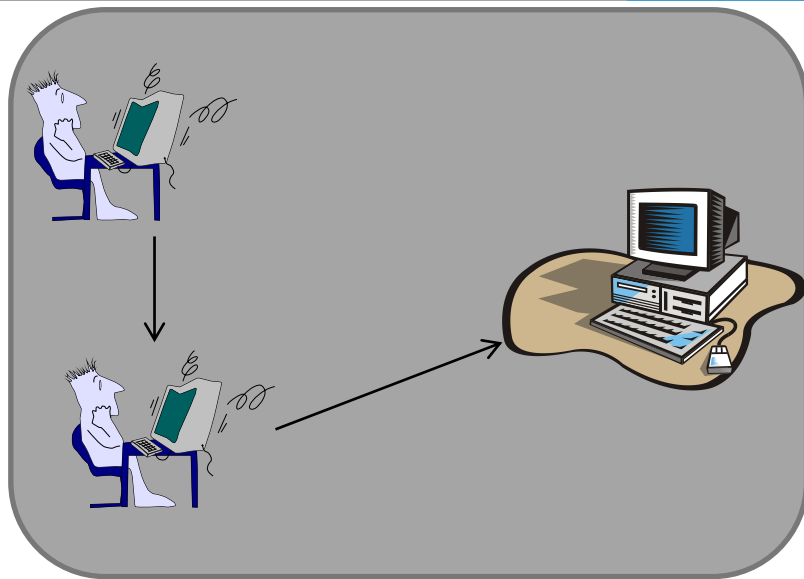
# 跨站脚本攻击

## ❖ 跨站脚本的类型

- 反射型 (reflected XSS)
- 存储型 (stored XSS)
- 基于DOM (DOM-basic)

## ❖ 跨站脚本威胁

- 敏感信息泄露
- 账号劫持、Cookie欺骗
- 拒绝服务
- 钓鱼
- .....



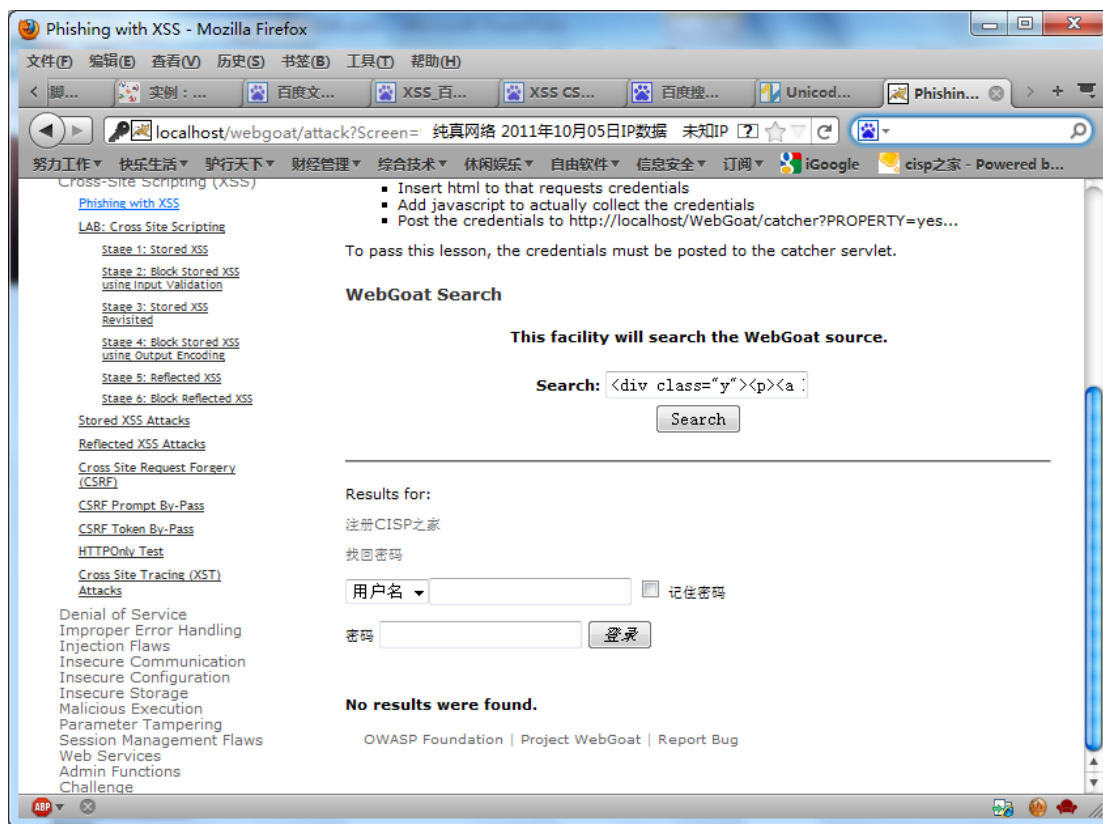




# 跨站脚本范例-页面嵌入

## ❖ 使用跨站脚本进行钓鱼攻击

- 提交脚本
- 欺骗性信息
- 用户信任

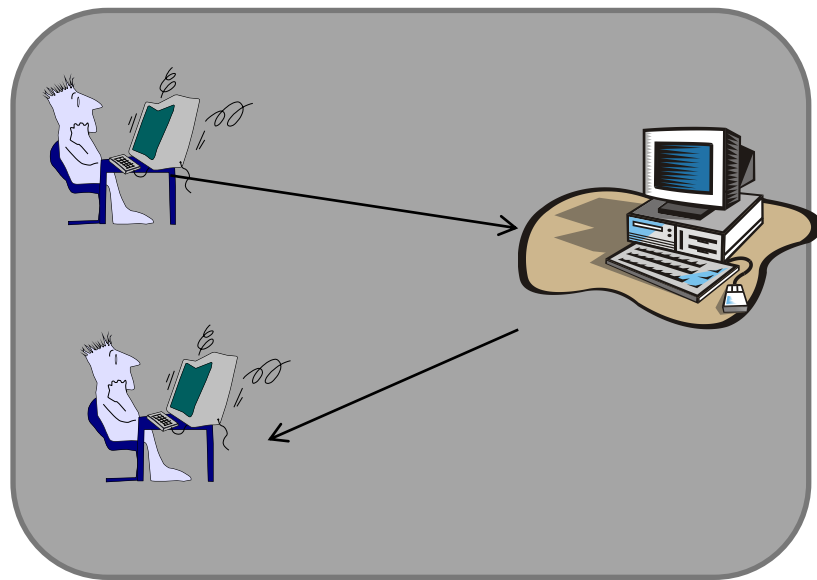




# 跨站脚本范例-信息窃取

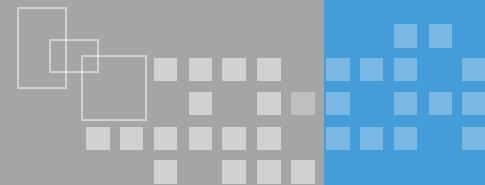
## ❖ 使用跨站脚本窃取敏感信息

- 用户构建窃取管理员信息的脚本，如论坛帖子、留言板等
- 要求管理员访问，如论坛帖子为“管理员请进来看看！”
- 管理员访问后，session 等敏感信息别窃取
- 伪造管理员进行登录





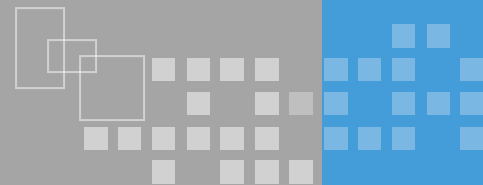
# 跨站脚本攻击的防范



- ❖ 跨站脚本问题与SQL注入漏洞类似，都是利用程序员编写脚本或页面过滤不足所导致
- ❖ 相对SQL注入而言，跨站脚本安全问题和特点更复杂，这使得对跨站脚本漏洞的防范难度更大。
- ❖ 对于用户可提交的信息要进行严格的过滤，防止跨站脚本漏洞的产生。



# 后门-方便下次进入



## ❖ 后门可以作什么

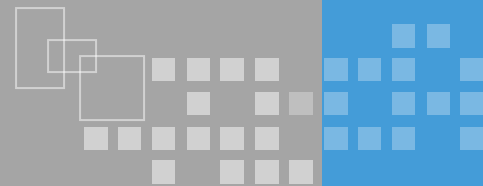
- 方便下次直接进入
- 监视用户所有行为、隐私
- 完全控制用户主机

## ❖ 后门放置方式


- 如果已经入侵
  - 简单！
- 如果尚未入侵
  - 手动放置
  - 利用系统漏洞，远程植入
  - 利用系统漏洞，诱骗执行



# 后门-方式



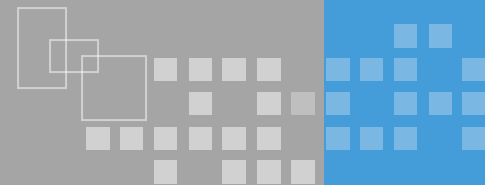
- ❖ 特洛伊木马
  - 随系统自启动
    - 修改注册表
    - 服务
    - Ini文件
- ❖ RootKit
  - 设备驱动
- ❖ 脚本后门
  - 难以查找
- ❖ 隐藏账号
  - 考验管理人员耐心与细心



相关知识  
参考恶意  
代码课程!



# 日志-抹去痕迹



## ❖ 清除/改写日志

### ■ 日志存放路径

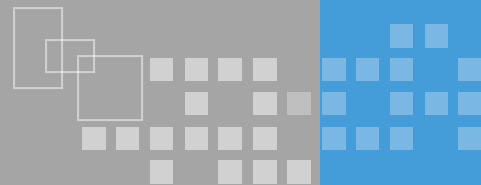
- 例如：IIS访问日志位置

`%WinDir%\System32\LogFiles\W3SVC1\exyymmdd.log`

### ■ 修改系统日期

## ❖ 删除中间文件

## ❖ 删除创建的用户



## ❖ 日志设置

- 尽可能多的信息
- 日志时间
- 日志空间

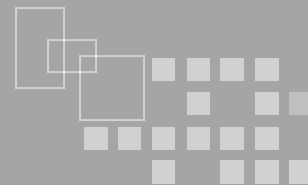
## ❖ 日志权限

## ❖ 日志存储

- 本地路径及备份方式
- 网络存储（日志服务器）



# 日志分析重点



- ❖ 日期 时间 (确定攻击的时间)
- ❖ 源IP (确定攻击者IP)
- ❖ 请求方法 (部分情况下要关注post操作)
- ❖ 请求链接 (查找链接中的特殊字符串)
- ❖ 状态代码 (了解操作的结果)





- ## ❖ 关注记录中的非正常编码

- 例如红色代码蠕虫攻击会形成如下记录

[illegible]

## ❖ 关注日志请求链接中的关键字

- cmd、select、xp\_cmdshell、Post等



**谢谢，请提问题！**