启明星辰认证安全技术工程师培训
---黑客攻击技术

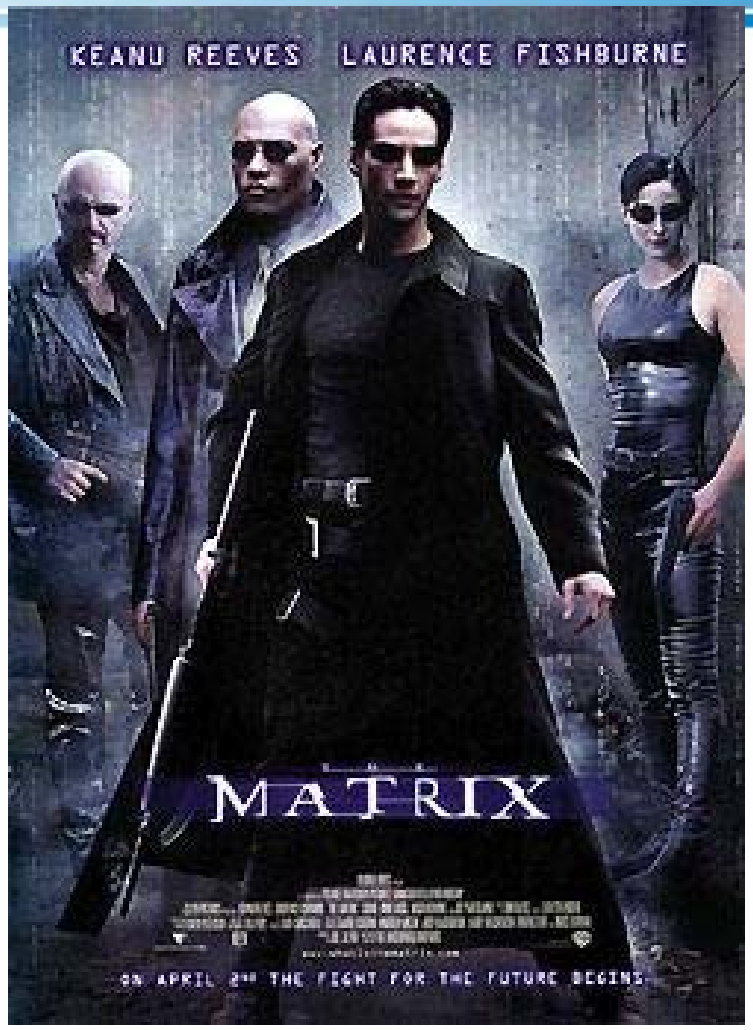
网 络 光 明 的 使 者

黑客攻击技术

- 黑客简史
- 黑客攻击分类
- 黑客攻击的一般过程
- 常见黑客攻击手段

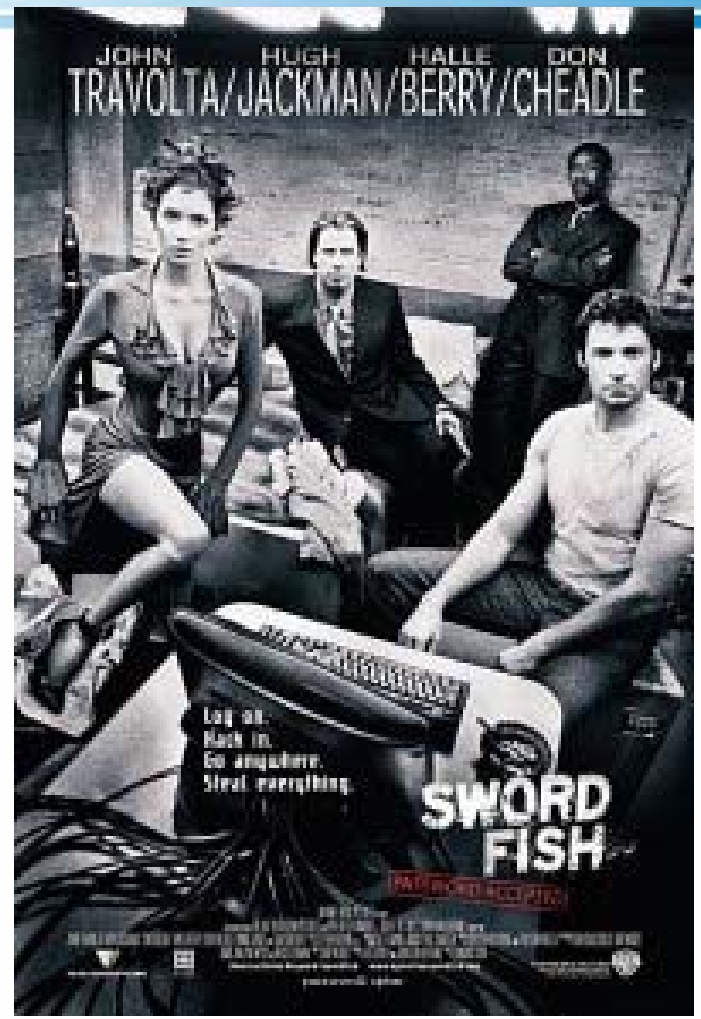
黑客究竟是什么？

电影媒体眼中的黑客形象



黑客帝国

浪漫主义的黑客电影



箭鱼行动

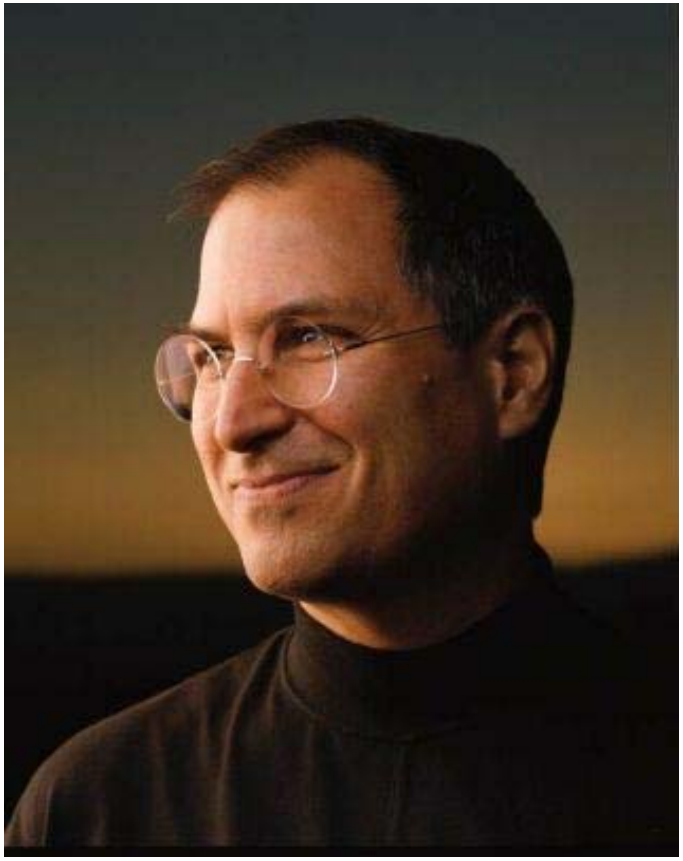
写实主义的黑客电影

黑客起源的背景

- ✓起源地：
  - 美国
- ✓精神支柱：
  - 对技术的渴求
  - 对自由的渴求
- ✓历史背景：
  - 越战与反战活动
  - 马丁·路德金与自由
  - 嬉皮士与非主流文化
  - 电话飞客与计算机革命

黑客？创新者

✓伍兹尼亚克和乔布斯



✓艾伦与盖茨

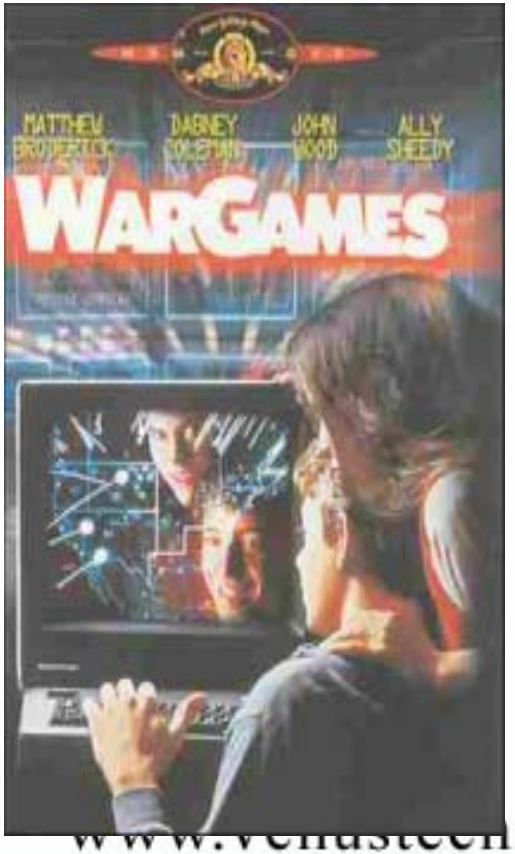
黑客？嬉皮士

- ✓艾比·霍夫曼
  - 嬉皮士之易比派（Yippies）
  - 举起五角大楼行动
- ✓电话飞客
  - 蓝匣子
  - **1990年AT&T瘫痪事件**

黑客？攻击者

✓罗伯特·莫里斯

✓凯文·米特尼克

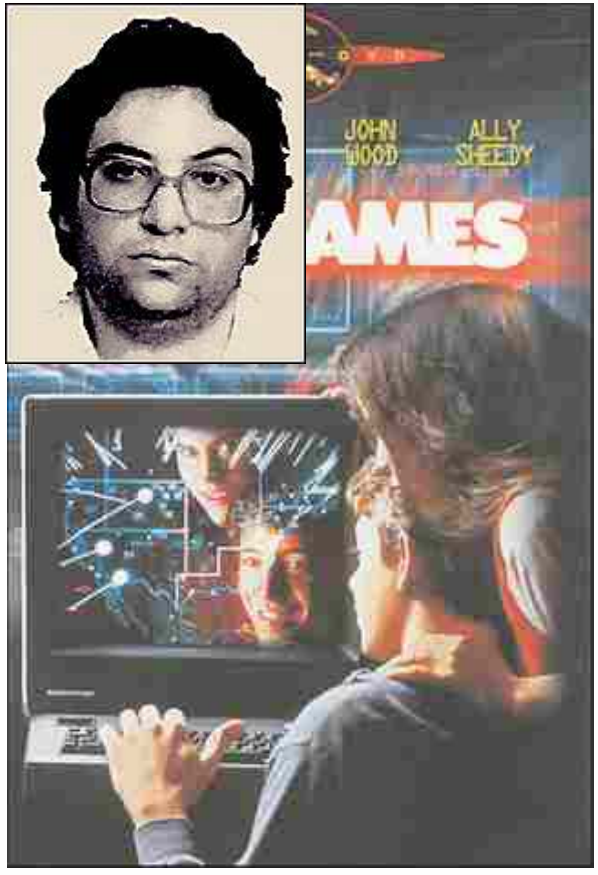


罗伯特•莫里斯

- 1988年，莫里斯蠕虫病毒震撼了整个世界。由原本寂寂无名的大学生罗伯特·莫里斯制造的这个蠕虫病毒入侵了大约6000个大学和军事机构的计算机，使之瘫痪。此后，从CIH到美丽杀病毒，从尼姆达到红色代码，病毒、蠕虫的发展愈演愈烈。

凯文•米特尼克

- ✓ 凯文•米特尼克是美国20世纪最著名的黑客之一，他是《社会工程学》的创始人
- ✓ 1979年他和他的伙伴侵入了北美空防指挥部。
- ✓ 1983年的电影《战争游戏》演绎了同样的故事，在片中，以凯文为原型的少年黑客几乎引发了第三次世界大战。



中国的“黑客文化”

- ✓中国缺乏欧美抚育黑客文化的土壤
  - 缺少庞大的中产阶层
  - 缺少丰富的技术积累
- ✓中国的黑客文化更多带有“侠”的色彩
  - 侠之大者，为国为民
  - 侠之小者，除暴安良

中国“黑客”重要历史事件

- ✓1998年印尼事件
- ✓1999年南联盟事件
- ✓2000年安氏网站被黑事件
- ✓绿色兵团南北分拆事件
- ✓中美五一黑客大战事件

黑客的分类

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 - 袁哥等
软件破解 - 0 Day
工具提供 - Numega

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 - 陈英豪
攻击Yahoo者 -匿名

黑客攻击技术

- 黑客简史
- 黑客攻击分类
- 黑客攻击的一般过程
- 常见黑客攻击手段

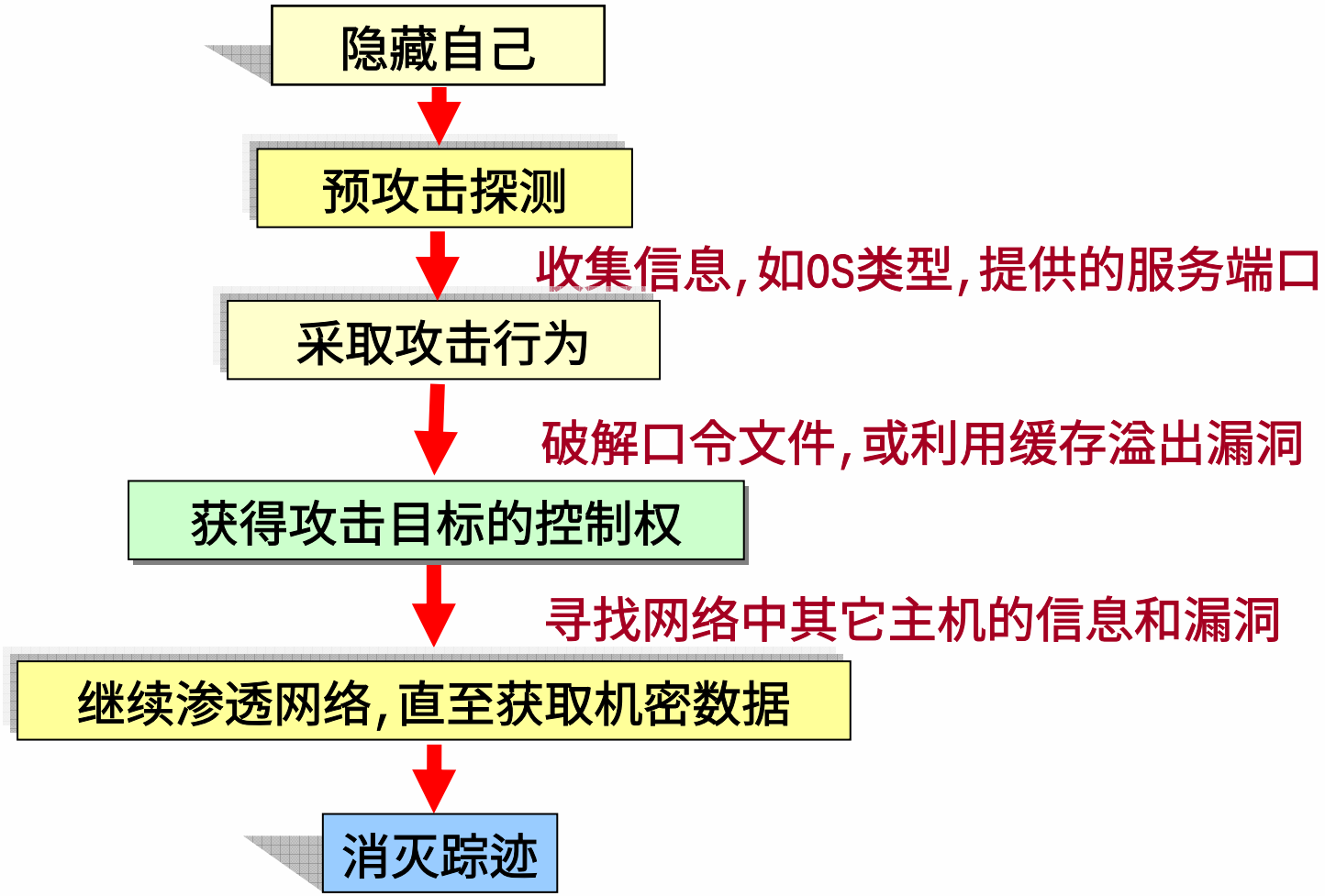
黑客攻击分类

- 被动攻击
- 主动攻击
- 物理临近攻击
- 内部人员攻击
- 软硬件装配分发攻击

黑客攻击技术

- 黑客简史
- 黑客攻击分类
- 黑客攻击的一般过程
- 常见黑客攻击手段

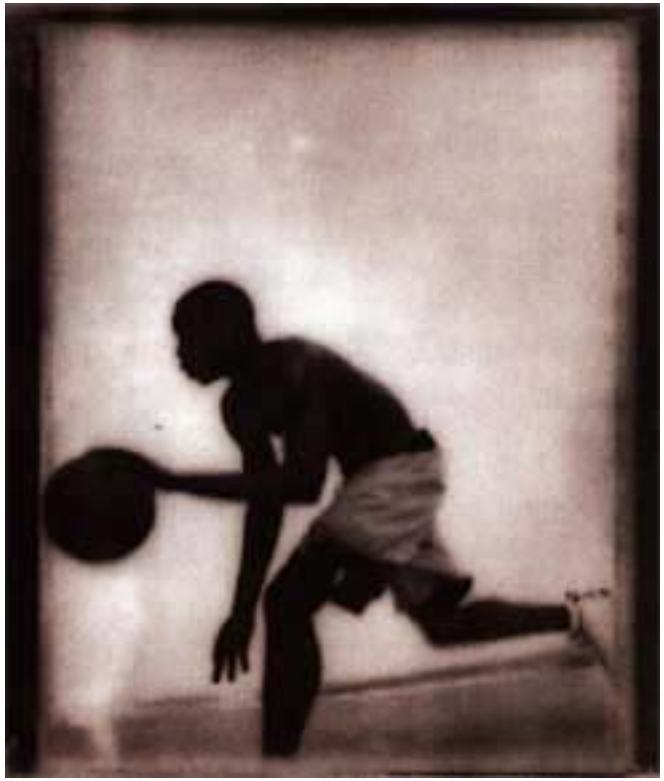
黑客攻击一般过程


隐藏自己
预攻击探测
收集信息,如OS类型,提供的服务端口
采取攻击行为
破解口令文件,或利用缓存溢出漏洞
获得攻击目标的控制权
寻找网络中其它主机的信息和漏洞
继续渗透网络,直至获取机密数据
消灭踪迹

黑客攻击一般过程

隐藏自己

- ✓ 从已经取得控制权的主机上通过 telnet或 rsh 跳跃
- ✓ 从 windows 主机上通过 wingates 等服务进行跳跃
- ✓ 利用配置不当的代理服务器进行跳跃
- ✓ 先通过拨号找寻并连入某台主机，然后通过这台主机



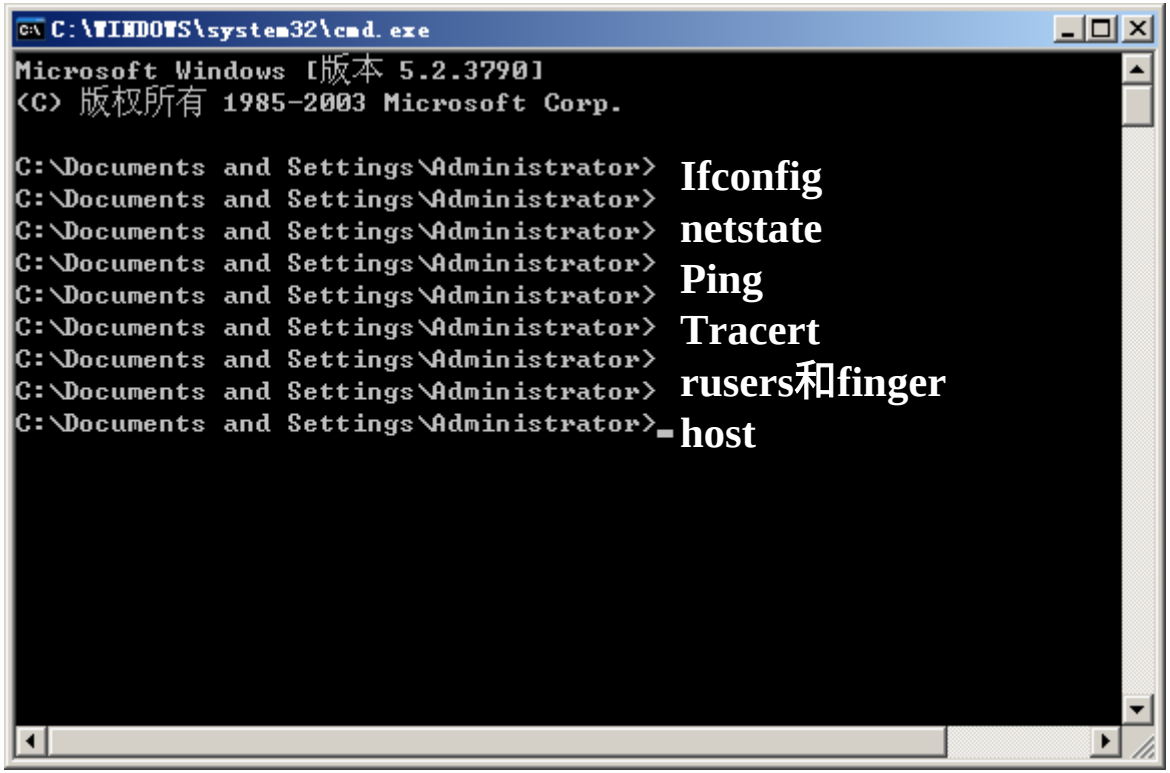
黑客攻击一般过程

预攻击探测

- ✓相关命令获取
- ✓手工获取banner
- ✓相关漏洞扫描工具

预攻击探测

相关网络命令



相关网络命令--Ping

Ping命令经常用来对TCP/IP网络进行诊断。通过向目标计算机发送一个ICMP数据包，目标计算机收到后再反送回来，如果返回的数据包和发送的数据包一致，就说明网络能够连通。通过Ping命令，可以判断目标计算机是否正在运行，以及网络的大致延时（数据包从发送到返回需要的时间）。

```
C:\>ping 192.168.0.162
Pinging 192.168.0.162 with 32 bytes of data:
Reply from 192.168.0.162: bytes=32 time<10ms TTL=128
Reply from 192.168.0.162: bytes=32 time<10ms TTL=128

C:\>ping 192.168.0.241
Pinging 192.168.0.241 with 32 bytes of data:
Reply from 192.168.0.241: bytes=32 time<10ms TTL=255
```

相关网络命令--finger

 # finger

user S00 PPP ppp-122-pm1.wiza Thu Nov 14 21:29:30 - still logged in

user S15 PPP ppp-119-pm1.wiza Thu Nov 14 22:16:35 - still logged in

user S26 PPP ppp-124-pm1.wiza Fri Nov 15 01:26:49 - still logged in

user S-1 0.0.0.0 Sat Aug 10 15:50:03 - still logged in

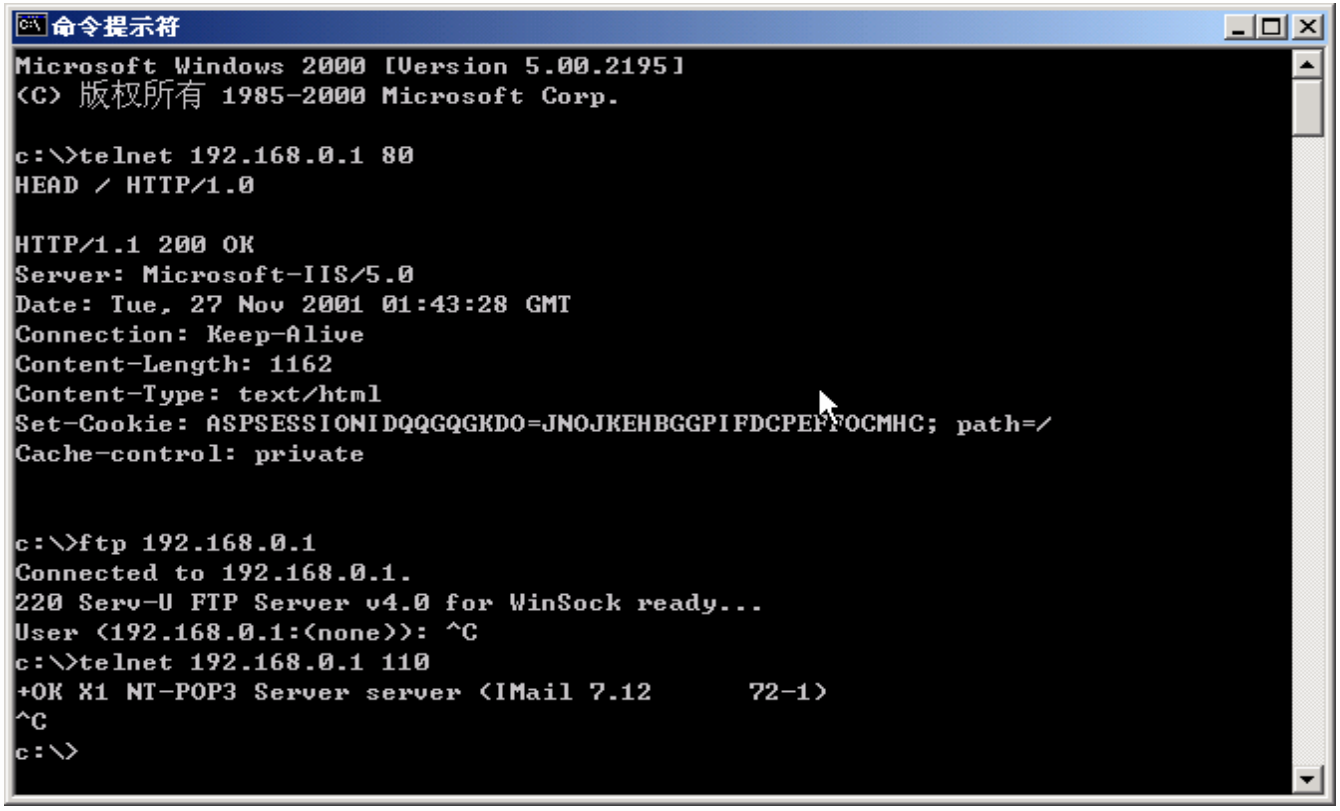
user S23 PPP ppp-103-pm1.wiza Fri Nov 15 00:13:53 - still logged in

黑客攻击一般过程

预攻击探测

- ✓相关命令获取
- ✓手工获取banner
- ✓相关漏洞扫描工具

手工获取Banner


命令提示符
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.
c:\>telnet 192.168.0.1 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 27 Nov 2001 01:43:28 GMT
Connection: Keep-Alive
Content-Length: 1162
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQQGQGKDO=JNOJKEHBGGPIFDCPEFFOCMHC; path=/
Cache-control: private
c:\>ftp 192.168.0.1
Connected to 192.168.0.1.
220 Serv-U FTP Server v4.0 for WinSock ready...
User (192.168.0.1:(none)): ^C
c:\>telnet 192.168.0.1 110
+OK X1 NT-POP3 Server server (IMail 7.12 72-1)
^C
c:\>

网络信息收集方式

- ✓ **Ping Sweep**
- ✓ **Dns Sweep**
- ✓ **Snmp Sweep**
- ✓ **Tracert**
- ✓ **Nslookup（zone transfer）**
- ✓ **浏览器**
- ✓ **NETCRAFT\WHOIS**
- ✓ **rusers和finger**

黑客攻击一般过程

预攻击探测

- ✓相关命令获取
- ✓手工获取banner
- ✓相关漏洞扫描工具

演示扫描

网络漏洞扫描

- ✓**NMAP**
- ✓**NESSUS**
- ✓**NIKTO**
- ✓**X-SCAN**
- ✓**RETINA**

黑客攻击的一般过程

消灭踪迹

- ✓删除添加的帐号
- ✓删除/修改日志
- ✓删除临时使用文件

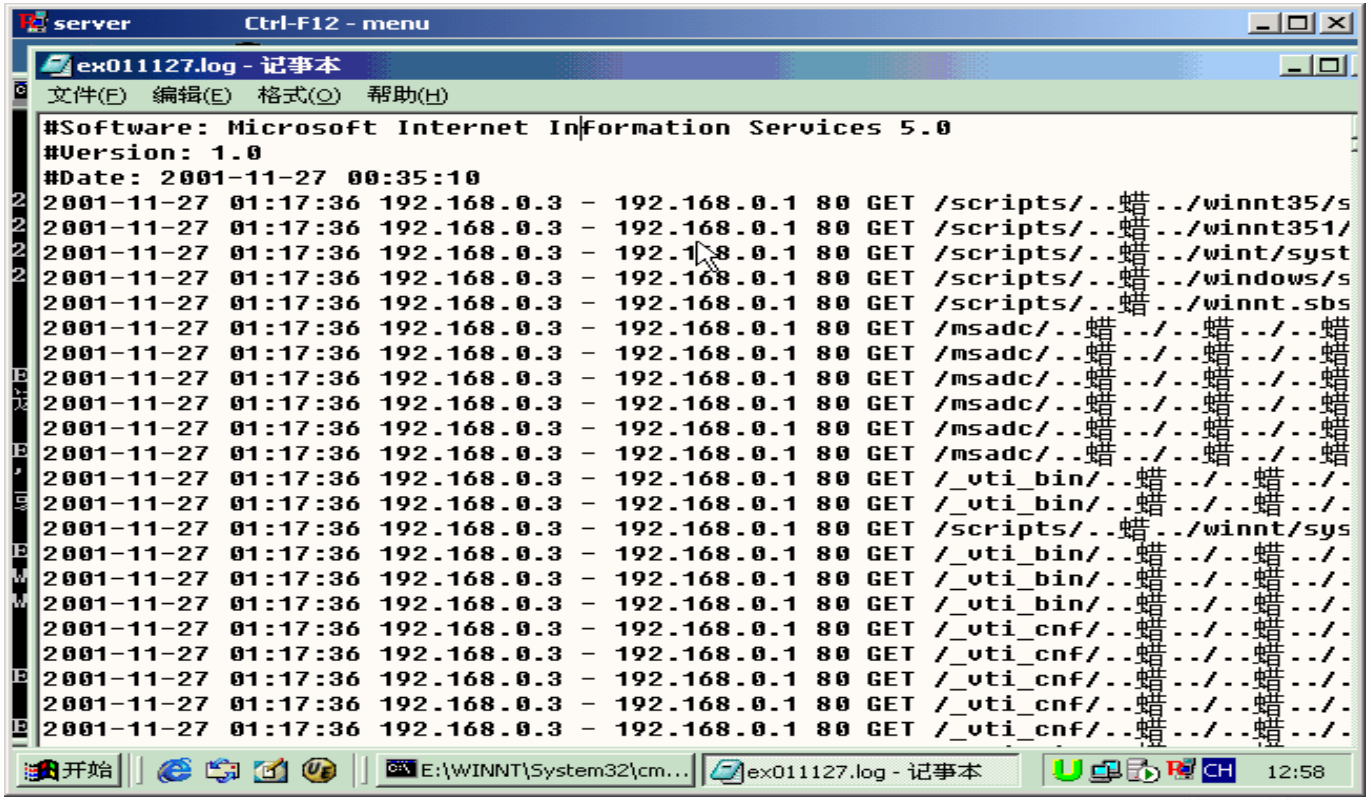
消灭踪迹

✓删除临时账号hacker

C:\>net user hacker /del

消灭踪迹

✓删除或修改日志



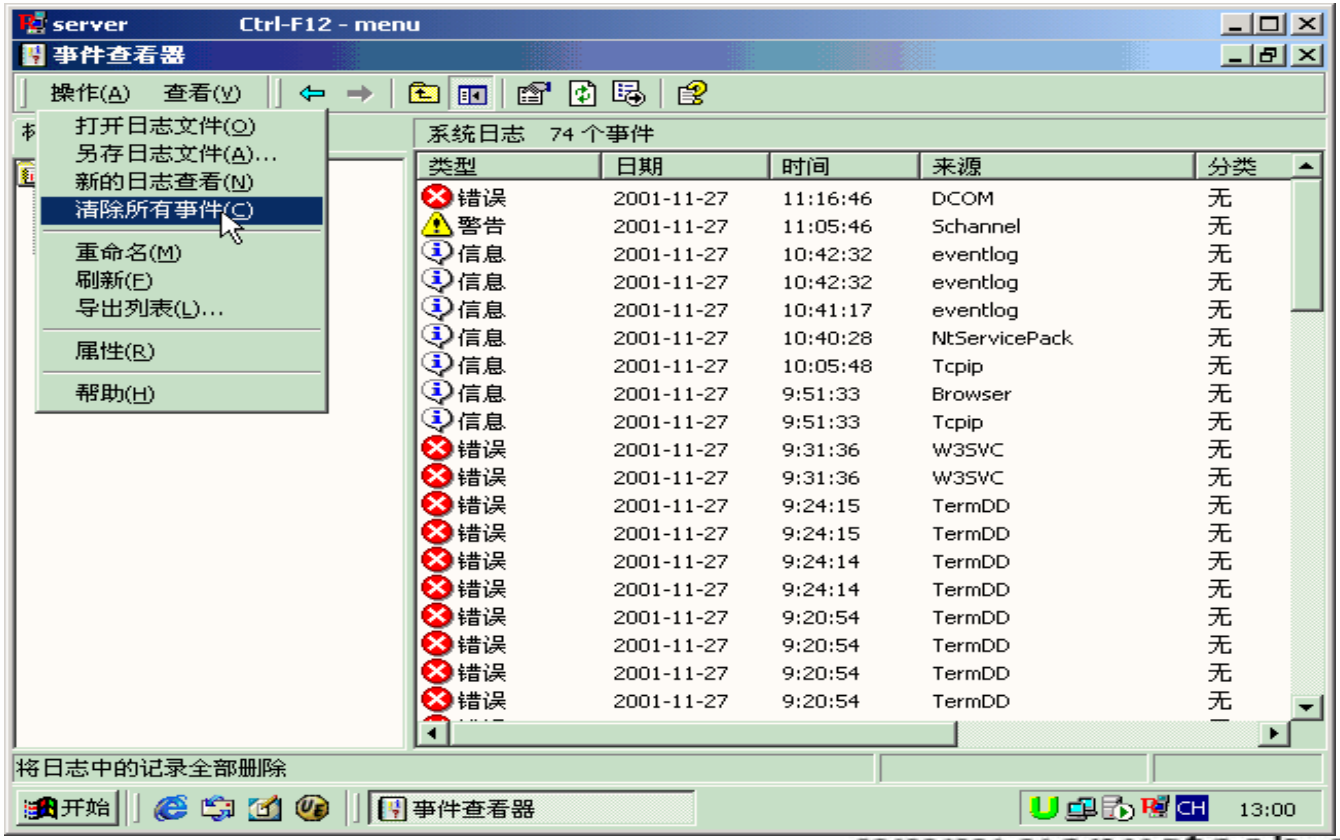
消除踪迹

✓删除临时上传文件

C:\>del WHOAMI.EXE

消灭踪迹

✓清除系统事件


server Ctrl-F12 - menu
事件查看器
操作(A) 查看(V)
打开日志文件(O)
另存日志文件(A)...
新的日志查看(N)
清除所有事件(C)
重命名(M)
刷新(F)
导出列表(L)...
属性(R)
帮助(H)
系统日志 74 个事件
类型 日期 时间 来源 分类
错误 2001-11-27 11:16:46 DCOM 无
警告 2001-11-27 11:05:46 Schannel 无
信息 2001-11-27 10:42:32 eventlog 无
信息 2001-11-27 10:42:32 eventlog 无
信息 2001-11-27 10:41:17 eventlog 无
信息 2001-11-27 10:40:28 NtServicePack 无
信息 2001-11-27 10:05:48 Tcpip 无
信息 2001-11-27 9:51:33 Browser 无
信息 2001-11-27 9:51:33 Tcpip 无
错误 2001-11-27 9:31:36 W3SVC 无
错误 2001-11-27 9:31:36 W3SVC 无
错误 2001-11-27 9:24:15 TermDD 无
错误 2001-11-27 9:24:15 TermDD 无
错误 2001-11-27 9:24:14 TermDD 无
错误 2001-11-27 9:24:14 TermDD 无
错误 2001-11-27 9:20:54 TermDD 无
错误 2001-11-27 9:20:54 TermDD 无
错误 2001-11-27 9:20:54 TermDD 无
错误 2001-11-27 9:20:54 TermDD 无
将日志中的记录全部删除
开始
事件查看器
CH
13:00

消灭踪迹

- ✓ **Windows日志**
  - 应用程序日志
  - 安全日志
  - 系统日志
  - 计划任务日志
  - **IIS等应用日志**

消灭踪迹

✓UNIX系统日志

日志文件	目　标
access-log	记录HTTP/web的传输
acct/pacct	记录用户命令
aculog	记录调制解调器的活动
btmp	记录失败的登录
lastlog	记录最近几次成功登录的时间和最后一次不成功的登录
messages	从syslog中记录信息（通常链接到syslog文件）
sudolog	记录使用sudo发出的命令
sulog	记录su命令的使用
syslog	从syslog中记录信息（通常链接到message文件）
utmp	记录当前登录的每个用户
wtmp	一个用户每次登录进入和退出时间的永久记录
xferlog	记录FTP会话

黑客攻击技术

- 黑客简史
- 黑客攻击分类
- 黑客攻击的一般过程
- 常见黑客攻击手段

常见攻击行为

- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓嗅探**sniffer**
- ✓社会工程

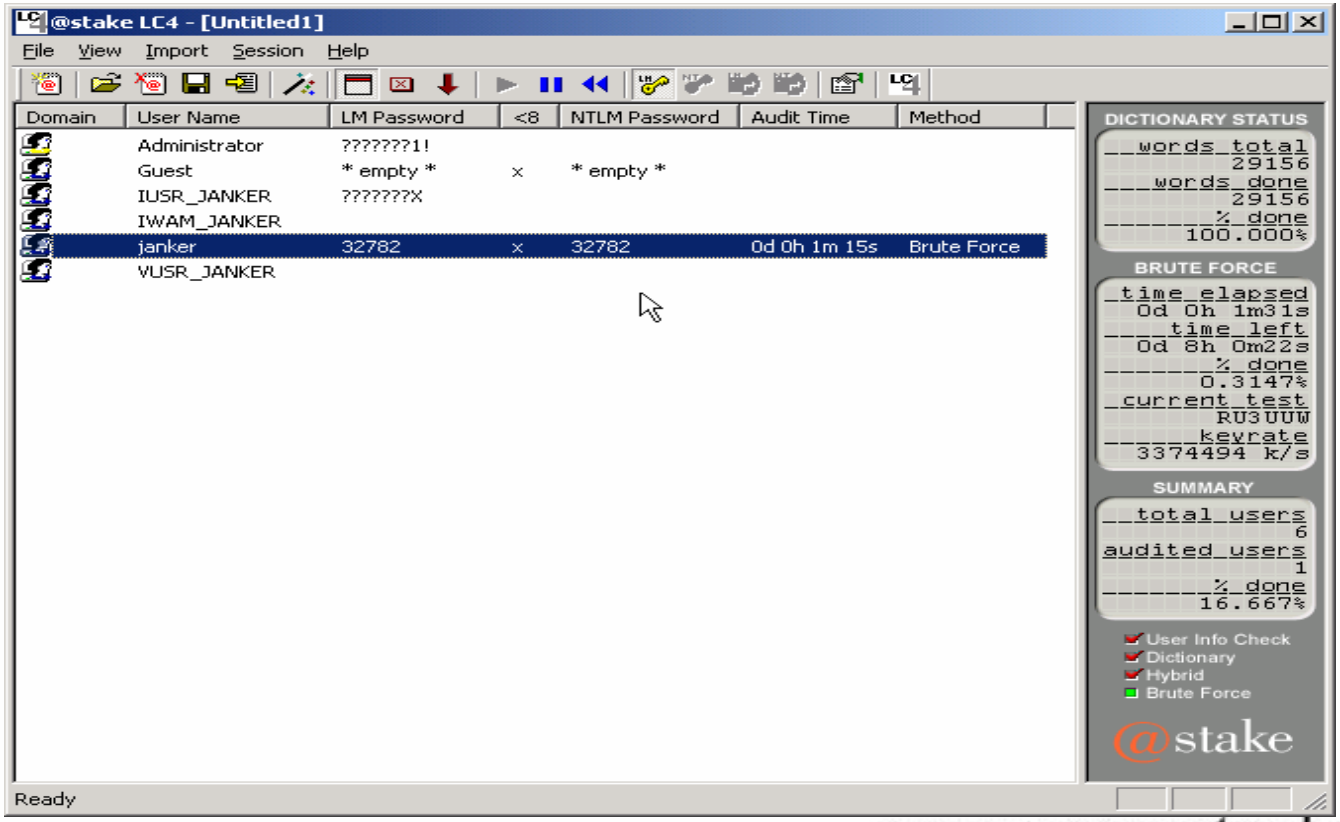
暴力猜解

暴力猜解就是从口令侯选器中一一选取单词，或用枚举法选取，然后用各种同样的加密算法进行加密再比较。一致则猜测成功，否则再尝试。

- ✓ 口令候选器
- ✓ 枚举法
- ✓ 口令加密
- ✓ 口令比较
- ✓ 获取口令的方法
- ✓ 防御方法

暴力猜解攻击

✓攻击实例：破解Win2000用户密码



暴力猜解

✓可被猜解的协议

- **Telnet、Ftp、Ssh、Rexec**
- **Http、Https、Nntp、Cvs**
- **Http-Proxy、Socks5**
- **LDAP、SMB、AAA**
- **Smtp、Pop3、Imap、Snmp**
- **Ms-sql、My-sql**

常见攻击行为

- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓嗅探**sniffer**
- ✓社会工程

利用已知漏洞的攻击

一、配置不当

- ✓SQL Injection攻击
- ✓跨站脚本攻击
- ✓unicode编码二次漏洞
- ✓"read.php3"
- ✓Sql server 空口令

SQL Injection

- ✓SQL Injection 是指SQL 指令植入式攻击，主要是属于Input Validation（输入验证） 的问题。
- ✓一个利用写入特殊SQL程序代码攻击应用程序的动作。
- ✓影响的系统包括MSSQL、MySQL、Oracle、Sybase与DB2等。

SQL Injection原理

- select * from member where UID =‘ “& request(”ID“) &”’ And Passwd=‘ “& request(”Pwd“) & ”’
- 如果正常使用者帐号是A123456789，密碼1234，则 select * from member where UID ='A123456789' And Passwd='1234'　输入的帐号与密码等资料会取代ASP(or PHP、JSP)中的变量，并由两个单引号(' ')所包住，即：
- select * from member where UID =' "& request("ID") &"' AndPaswd=' "& request("Pwd") & "'

攻击实例

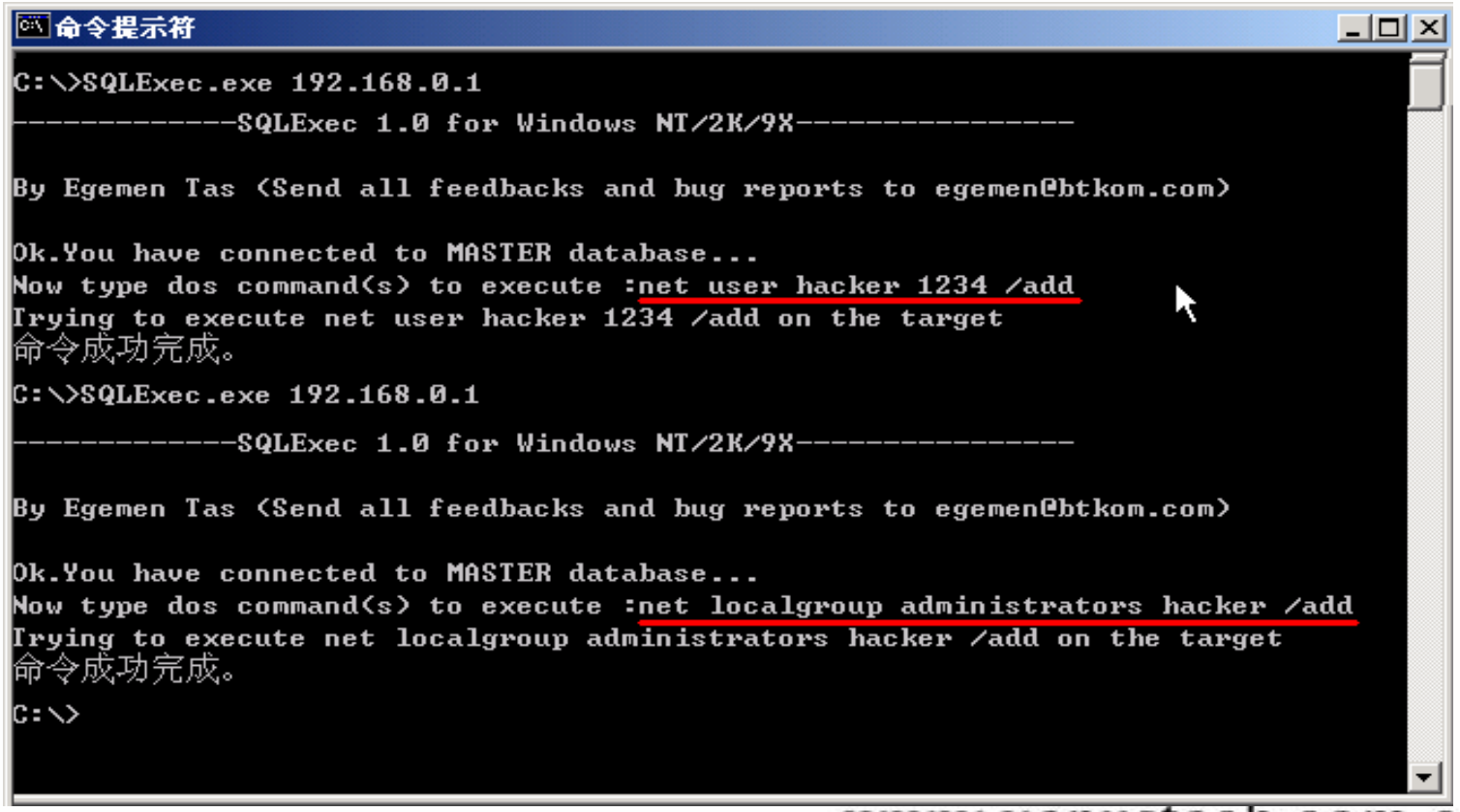
- ✓可以输入用户名**abcdefg(任意输入)**，密码**asdf(任意输入)'or 1=1**
- ✓即后台的语句为**select * from member where UID ='abcdefg' AndPasswd= 'asdf' or 1=1 --'**，则攻击者可以轻易进入系统。

防止SQL Injection

- ✓ 可以过滤输入条件中可能隐含的sql指令，如INSERT、SELECT、UPDATE等针对输入条件进行规范，如无必要，应改为仅可接受大小写英文字母与数写等。
- ✓ 针对特殊的查询参数进行过滤，如--、‘ 等可利用replace(xx, “ ’ ”, “ ‘’ ”)进行替换，
- ✓ 在程序编写时，应时常检查程序是否存在有非预期输入资料的漏洞。

利用漏洞攻击

✓尝试MSSQLServer管理员sa的空密码



利用已知漏洞的攻击

二、缓冲区溢出

- ✓远程溢出攻击
  - Windows RPC-DCOM、LSASS、NetDDE
  - IIS Webdav、.asp、.htr、.ida、.idq、.printer
  - MSSQL 2000/MSDE Hello/Resolution Overflow
  - Wu-ftp、Ws-ftp、Serv-u
  - Apache Chunked Encoding
  - Solaris telnetd、Dtspcd、sadmind、DistCC
- ✓本地溢出
  - 内核溢出
  - 应用溢出
  - 权限配置不当

缓冲区溢出攻击

缓冲区溢出技术原理

✓缓冲区溢出分类

---基于栈的缓冲区溢出

---格式串溢出

---基于堆的缓冲区溢出

✓防范缓冲区溢出

缓冲区溢出攻击

✓缓冲区溢出技术原理

通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的 。

缓冲区溢出分类

✓ 内存的概念

缓冲区溢出分类

✓例：基于栈的缓冲区溢出

栈是程序的临时变量的存储区域。一个简单的栈溢出的例子：

```
int main(int argc, char **argv)
{
  char buffer[16];  // 存储在Stack
  strcpy(buffer,argv[1]); //strcpy拷贝没有检测argv[1]参数的长度
                          //导致溢出
}
```

缓冲区溢出分类

- ✓ 基于栈的缓冲区溢出

  程序执行流程：

  压入当前的指令(寄存器(IP)作为函数返回的地址(ret)

  压入当前的栈帧ebp寄存器

  给局部变量分配空间(sub $0x10,%esp)

  [局部变量 16 字节][ebp 4字节][ret 4字节]

  |----填充大于16字节的数据导致溢出-----|

阻止缓冲区溢出的方法

- ✓ 不使用不安全的数据拷贝函数
- ✓ 在往缓冲区中填充数据时必须进行边界检查。
- ✓ 尽量动态分配内存以存储数据，不要使用固定大小的缓冲区
- ✓ 使用进行边界检查的编译器
- ✓ 使用户堆栈段不可执行
- ✓ 程序尽量不设置**suid/sgid**属性

常见攻击行为

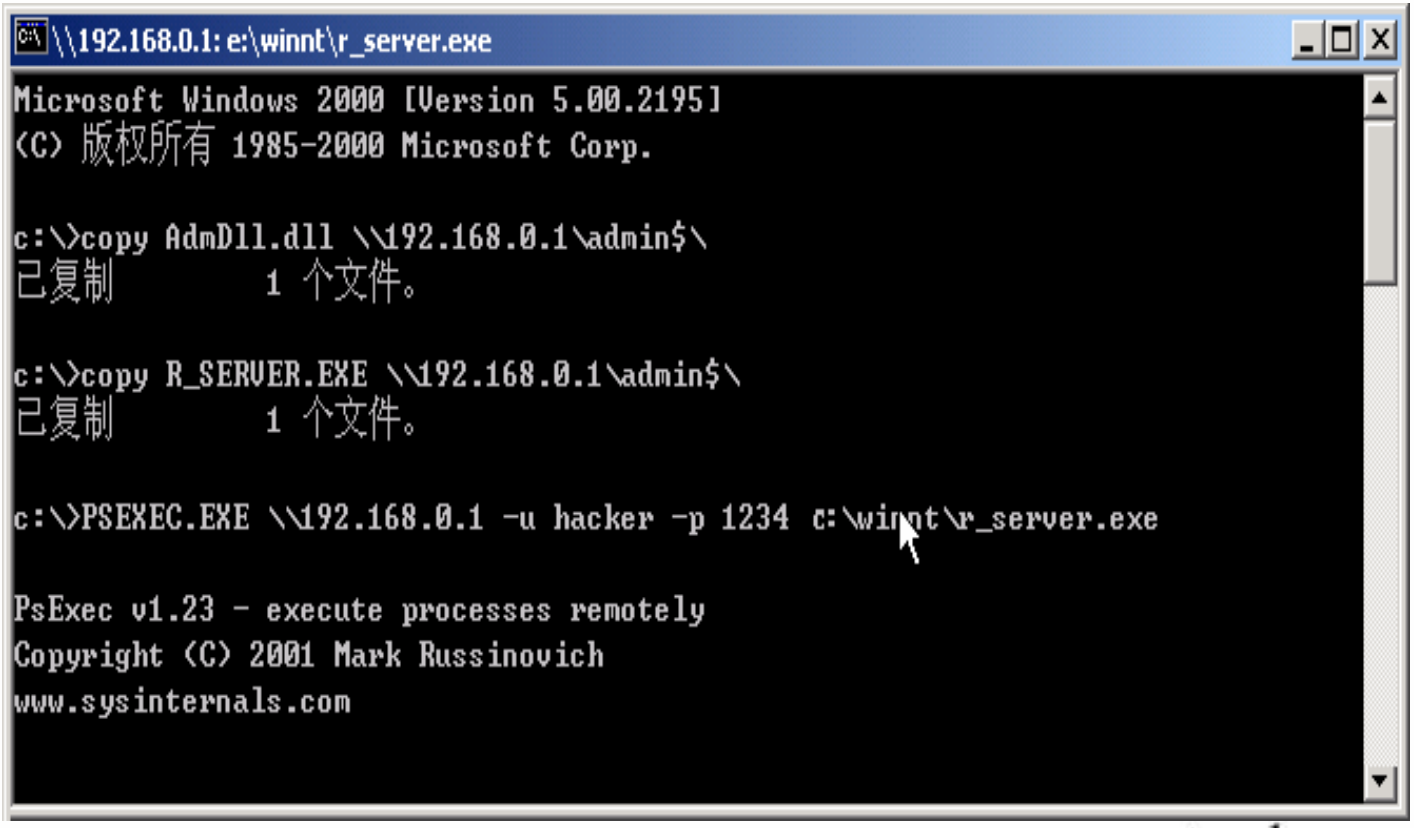
- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓嗅探**sniffer**
- ✓社会工程

什么是特洛依木马

- ✓“特洛伊木马”来源于希腊神话，讲述的是通过一个木马血屠特洛伊城的故事。这一故事形象地说明了木马程序的工作原理。
- ✓它一般有两个程序：一个是服务器端程序，一个是客户端程序。
- ✓服务器端程序的上传和自加载

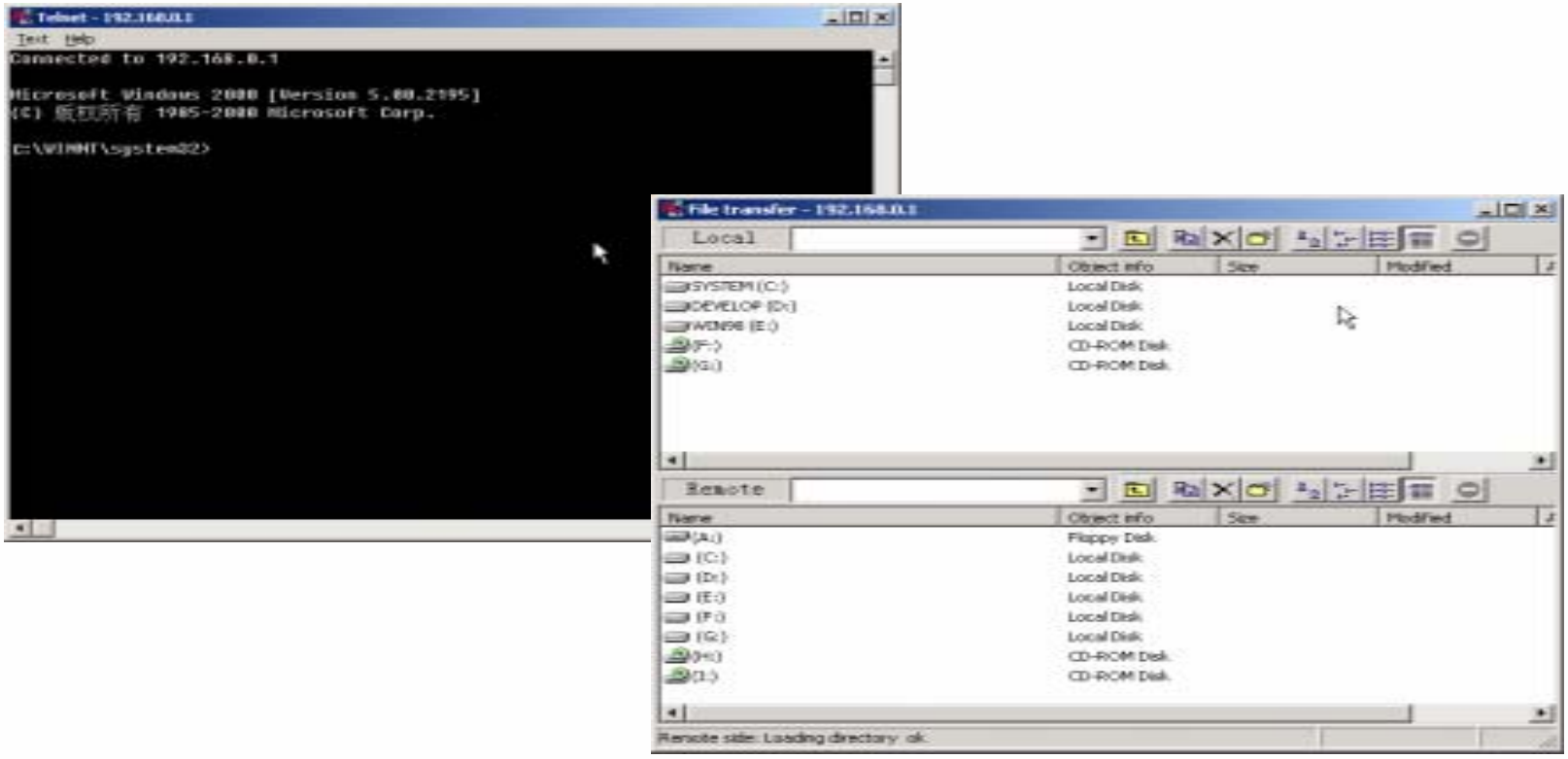
安装后门

✓上传并执行后门程序



安装后门

✓远程控制后门程序－Telnet/文件传输



后门攻击技术

·程序的自加载运行

加载程序到启动组

写程序启动路径到注册表的run

可以修改Boot.ini

通过注册表里的输入法键值直接挂接启动

通过修改Explorer.exe启动参数等

常见木马

常见攻击行为

- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓缓冲区溢出攻击
- ✓嗅探**sniffer**
- ✓社会工程

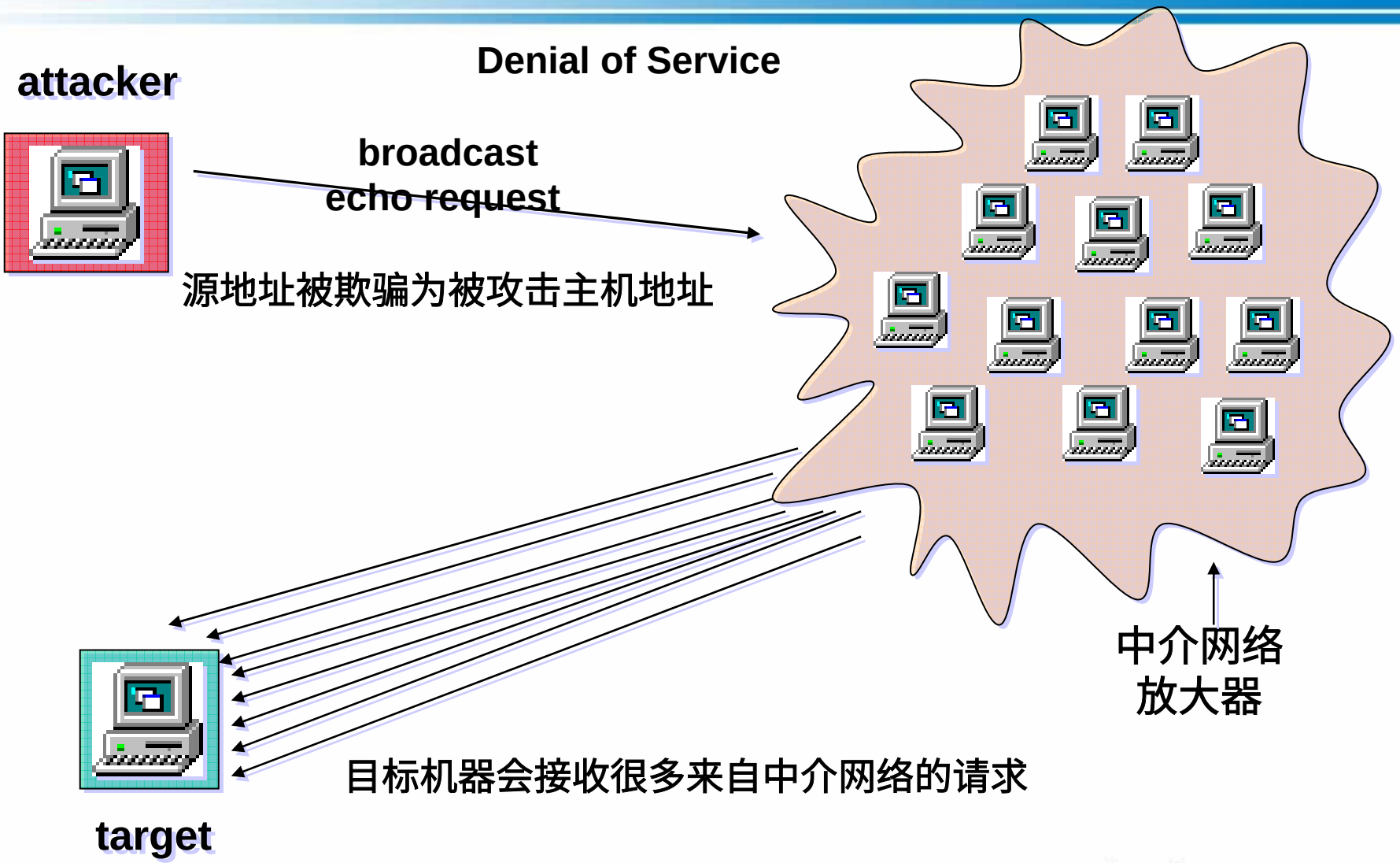
拒绝服务攻击

“拒绝服务攻击（Denial of Service）”的方法，简称DoS。它的恶毒之处是通过向服务器发送大量的虚假请求，服务器由于不断应付这些无用信息而最终筋疲力尽，而合法的用户却由此无法享受到相应服务，实际上就是遭到服务器的拒绝服务。

拒绝服务攻击--Smurf攻击

广播信息可以通过一定的手段（通过广播地址或其他机制）发送到整个网络中的机器。当某台机器使用广播地址发送一个ICMP echo请求包时（例如PING），一些系统会回应一个ICMP echo回应包，也就是说，发送一个包会收到许多的响应包。Smurf攻击就是使用这个原理来进行的，当然，它还需要一个假冒的源地址。也就是说在网络中发送源地址为要攻击主机的地址，目的地址为广播地址的包，会使许多的系统响应发送大量的信息给被攻击主机（因为他的地址被攻击者假冒了）。使用网络发送一个包而引出大量回应的方式也被叫做“放大器”。一些无能的且不负责任的网站仍有很多的这种漏洞。

拒绝服务攻击--Smurf攻击



Smurf 防御

- ✓Smurf的攻击平台
- ✓其路由器上启动了IP广播功能
- ✓将所有路由器上IP的广播功能都禁止

拒绝服务攻击--分布式拒绝服务

分布式拒绝服务

拒绝服务中更厉害的一种，叫分布式拒绝服务攻击（Distributed Denial of Service），简称DDoS。这些程序可以使得分散在互连网各处的机器共同完成对一台主机攻击的操作，从而使主机看起来好象是遭到了不同位置的许多主机的攻击。这些分散的机器由几台主控制机操作进行多种类型的攻击，如UDP flood, SYN flood等。

分布式拒绝服务

攻击入侵主机和安装程序的过程是完全自动化的，一般要经过四步：

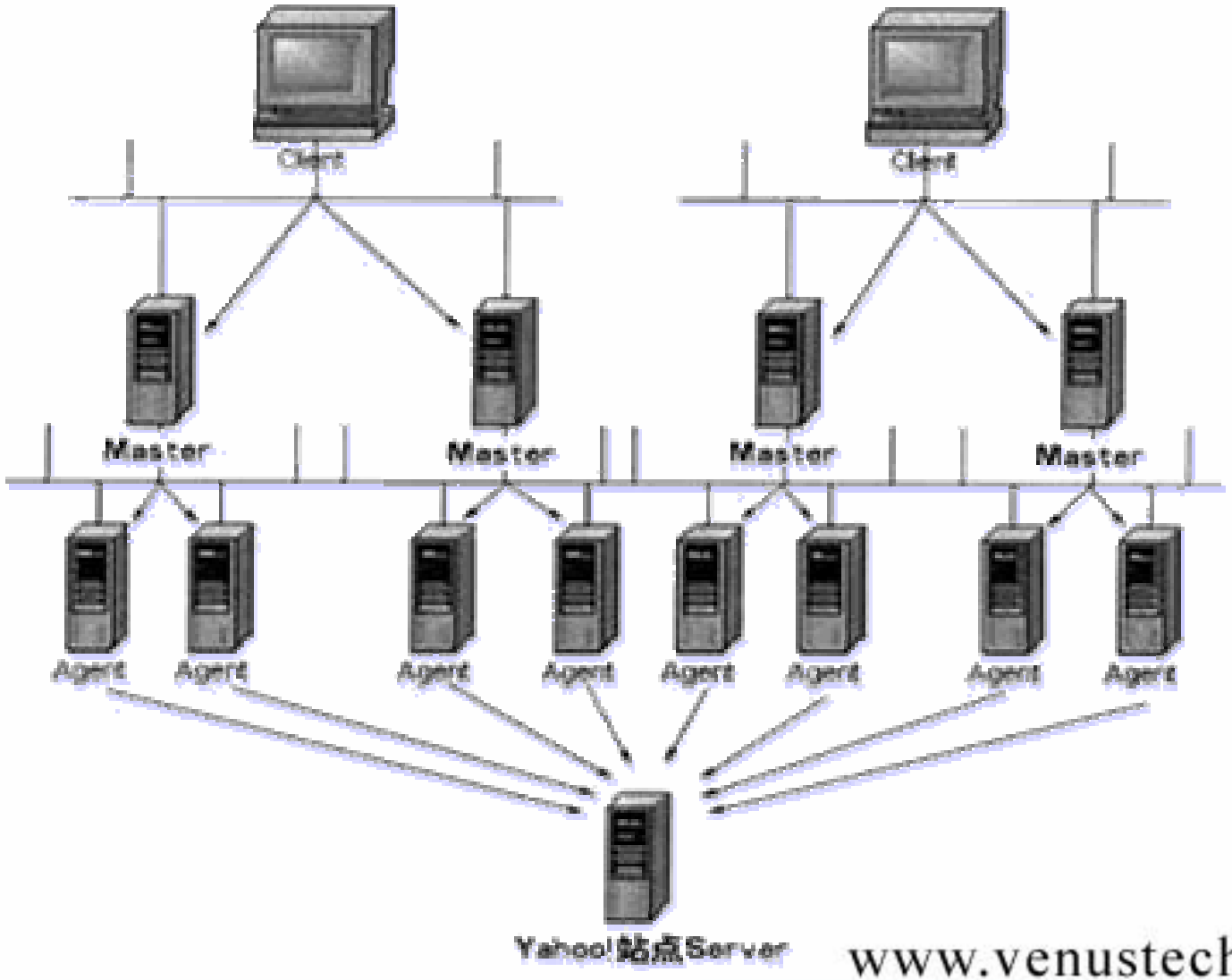
1．探测扫描大量主机以寻找可入侵的目标；

2．入侵有安全漏洞的主机并获取控制权，在每台入侵主机中安装攻击程序；

3．构造庞大的、分布式的攻网；

4．在同一时刻，由分布的成千上万台主机向同一目标地址发出攻击，目标系统全线崩溃。

实例：分布式拒绝服务攻击Yahoo！



术　　语

- ✓ 客户端——用于通过发动攻击的应用程序，攻击者通过它来发送各种命令。
- ✓ 守护程序——在代理端主机运行的进程，接收和响应来自客户端的命令。
- ✓ 主控端——运行客户端程序的主机。
- ✓ 代理端——运行守护程序的主机。
- ✓ 目标主机——分布式攻击的目标（主机或网络）。

防御方法

- ✓数据包过滤（包括特征分析）
- ✓利用syn-cookie,syn-cache
- ✓主动发送RST
- ✓断开网络
- ✓源追踪技术（traceback）
- ✓采用DDOS设备

对于TTL值的分析

- ✓ 系统默认的TTL值为255,128,64,32
- ✓ 通常的路由HOP为10-20
- ✓ 正常的TTL范围：235-245,108-118,44-54,12-22
- ✓ TFN3K的TTL算法

ttl=getrandom(200,255)

TTL的范围为：(MAX)180-245;(MIN)190-235

通过TTL值可过滤最大84.6%的攻击包

路由器上的配置

- ✓**Access-list访问控制列表**

access-list 101 deny ip 192.168.0.0 0.0.255.255.any

- ✓**Rate-limit 流量限制**

rate-limit output 512000...

transmit exceed-action drop

常见攻击行为

- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓**嗅探sniffer**
- ✓社会工程

Sniffer原理

一个网络接口应该只响应这样的两种数据帧：

1．与自己硬件地址相匹配的数据祯

2.发向所有机器的广播数据帧。

网卡来说一般有四种接收模式：

1.广播方式：该模式下的网卡能够接收网络中的广播信息。

2.组播方式：设置在该模式下的网卡能够接收组播数据。

3.直接方式：在这种模式下，只有目的网卡才能接收该数据。

4.混杂模式：在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

Sniffer方式

- ✓共享式网络
  - 混杂模式
    - **sniffer、Dnsniff、Ethereal、IRIS**
- ✓交换式网络
  - **ARP欺骗**
    - **cain、ettercap**

Sniffer危害

- ✓ 可以捕获口令；
- ✓ 可以截获机密的或专有的信息；
- ✓ 可以被用来攻击相邻的网络或者用来获取更高级别的访问权限。

防止被sniffer

- ✓检查网络线路，确定各端口上没有sniffer设备
- ✓检查机器的网卡模式，在sniffer存在时，窃听机器的端口被改为混杂模式（promiscuous mode）
- ✓采用VPN或SSL/SSH对数据进行加密。
- ✓设计合理的拓朴结构。Sniffer无法穿过VLAN和路由器，网络分段越细，则安全程度越高
- ✓采用IP-MAC-端口的绑定。

常见攻击行为

- ✓暴力猜解
- ✓利用已知漏洞攻击
- ✓特洛伊木马
- ✓拒绝服务攻击
- ✓缓冲区溢出攻击
- ✓嗅探sniffer
- ✓社会工程

社会工程学

- ✓什么是社会工程学
- ✓社会工程学成立的背景
- ✓社会工程学的攻击
- ✓社会工程学的防范

社会工程学

- ✓社会工程指的是：导致人们泄漏信息或诱导人们的行为方式并造成信息系统、网络或数据的非授权访问、非授权使用、或非授权暴露的一切成功或不成功的尝试。
- ✓成立的背景：人的本性、商务环境

社会工程学攻击

- ✓ 攻击流程：信息收集→选择目标→实施攻击
- ✓ 攻击类型

(1) 基于受害者虚荣心和自负心理的攻击；

(2) 利用同情心和情感的攻击；

(3) 利用胁迫进行的攻击。

社会工程学的防范

- ✓策略、意识和教育
- ✓建立事故响应小组
- ✓测试预防程度
- ✓应用可能的技术和管理措施 （如：电话跟踪、确保物理安全、密级划分）

总结

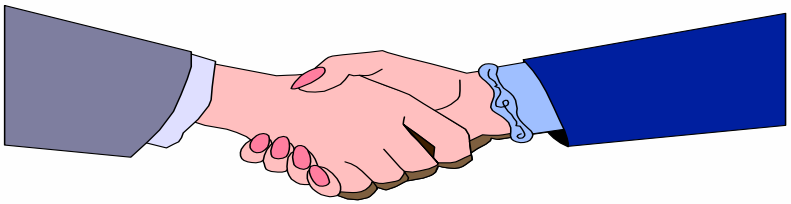
- 黑客简史
- 黑客攻击分类
- 黑客攻击的一般过程
- 常见黑客攻击手段

参考资料

- ✓ **http://www.venustech.com.cn**
- ✓ **http://www.xfocus.net**
- ✓ **http://www.securityfocus.com**
- ✓ **http://www.nsfocus.com**
- ✓ **http://www.microsoft.com**
- ✓ **http://www.linux.com**

Any questions?

谢谢大家



E-mail: train@venustech.com.cn