§8.1 黑客概述

- 黑客(Hacker)源于英语动词Hack，意为“劈、砍”，引申为“辟出、开辟”，进一步的意思是“干了一件非常漂亮的工作”。在20世纪早期的麻省理工学院校园口语中，黑客则有“恶作剧”之意，尤其是指手法巧妙、技术高明的恶作剧。
- 有一部分人认为，黑客是“热爱并精通计算机技术的网络狂热者”，并赋予他们“网上骑士”桂冠；相反，另一部分人则认为黑客是“企图非法获取计算机系统访问权的人”，甚至将其描述为“网络恐怖主义分子”；大多数人则认为，黑客是“试图通过网络非法获取他人计算机系统访问权并滥用计算机技术的人”。

§8.1 黑客概述

- 根据我国现行法律的有关规定，对黑客可以给出两个定义：
  - 广义的黑客是指利用计算机技术，非法侵入或擅自操作他人(包括国家机关、社会组织及个人)计算机信息系统，对电子信息交流安全具有不同程度的威胁性和危害性的人；
  - 狭义的黑客，是指利用计算机技术，非法侵入并擅自操作他人计算机信息系统，对系统功能、数据或者程序进行干扰、破坏，或者非法侵入计算机信息系统并擅自利用系统资源，实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的人。
  - 狭义的黑客包括在广义的黑客之中，前者基本上是计算机犯罪的主体，后者的行为不一定都构成犯罪。

§8.1 黑客概述



- 黑客守则

1、不要恶意破坏任何的系统，这样做只会给你带来麻烦。

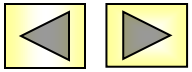
2、不要破坏别人的软件和资料。

3、不要修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，请在目的达到后将他改回原状。

4、不要轻易的将你要黑的或者黑过的站点告诉你不信任的朋友。

5、在发表黑客文章时不要用你的真实名字。

6、正在入侵的时候，不要随意离开你的电脑。



§8.1 黑客概述

- 黑客守则

7、不要入侵或破坏政府机关的主机。

8、将你的笔记放在安全的地方。

9、已侵入的电脑中的账号不得清除或修改。

10、可以为隐藏自己的侵入而作一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

11、不要做一些无聊、单调并且愚蠢的重复性工作。

12、做真正的黑客，读遍所有有关系统安全或系统漏洞的书。

§8.1 黑客概述

黑客入侵和破坏的危险

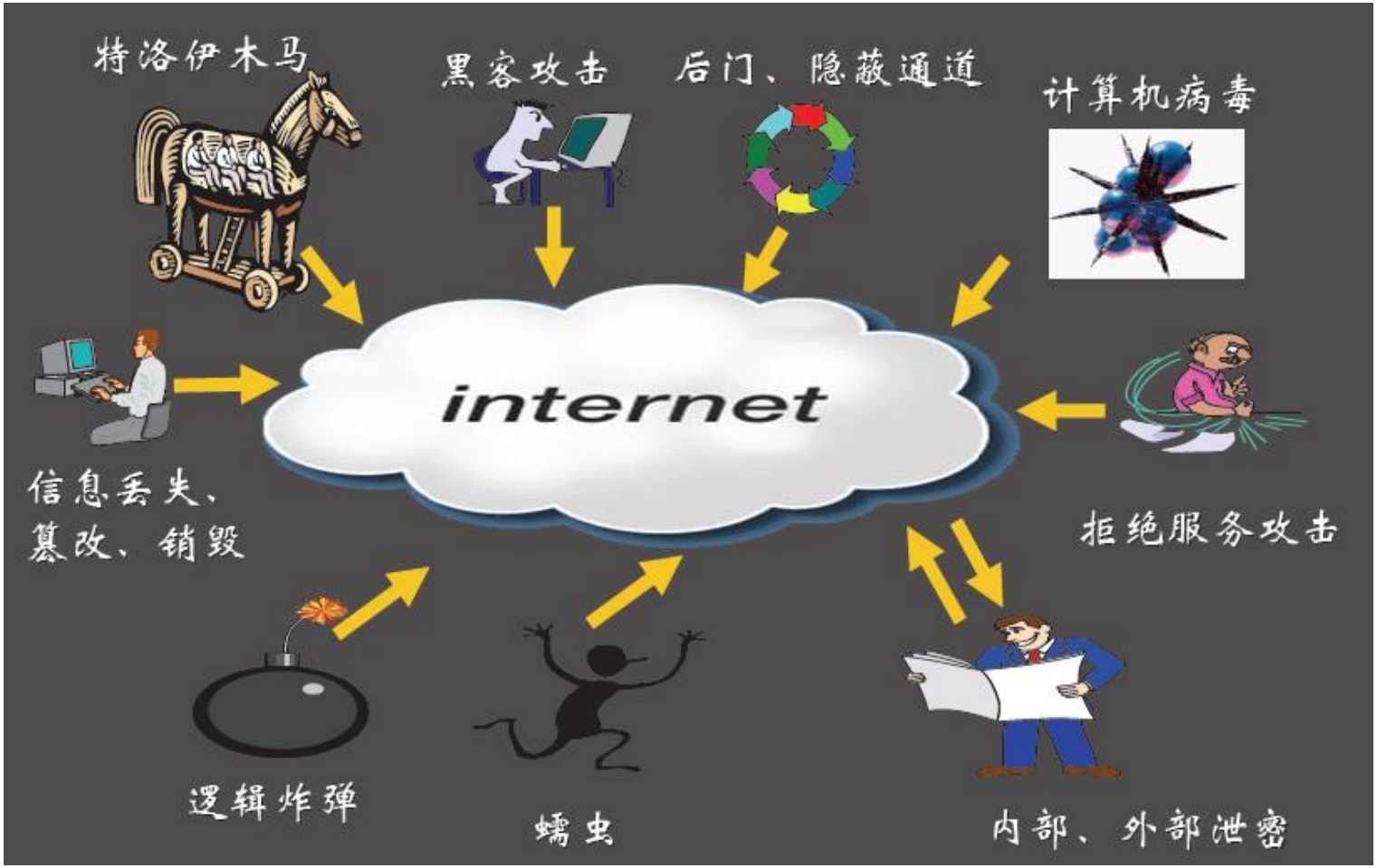
- 黑客”在网上的攻击活动每年以十倍速增长。
- 修改网页进行恶作剧、窃取网上信息兴风作浪。
- 非法进入主机破坏程序、阻塞用户、窃取密码。
- 串入银行网络转移金钱、进行电子邮件骚扰。
- 黑客可能会试图攻击网络设备，使网络设备瘫痪。

§8.1 黑客概述

- INTERNET 上有超过30,000 个黑客站点，下面是来自于黑客站点主页上的一些目录
  - 技术交流：为了兴趣和利益
  - 击破隐藏的口令保护
  - 发送EMAIL的漏洞列表
  - 如何成为一个UNIX黑客
  - 你曾经想成为特权用户吗
  - 怎样隐藏你的痕迹

§8.1 黑客概述

- 常见的黑客攻击类型



§8.1 黑客概述

- 典型的攻击步骤

预攻击探测 ← 隐藏自身

↓ 收集信息，如OS类型，提供的服务端口等

发现漏洞，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系统

↓ 获得系统帐号权限，并提升为root权限

安装系统后门

↓ 方便以后使用

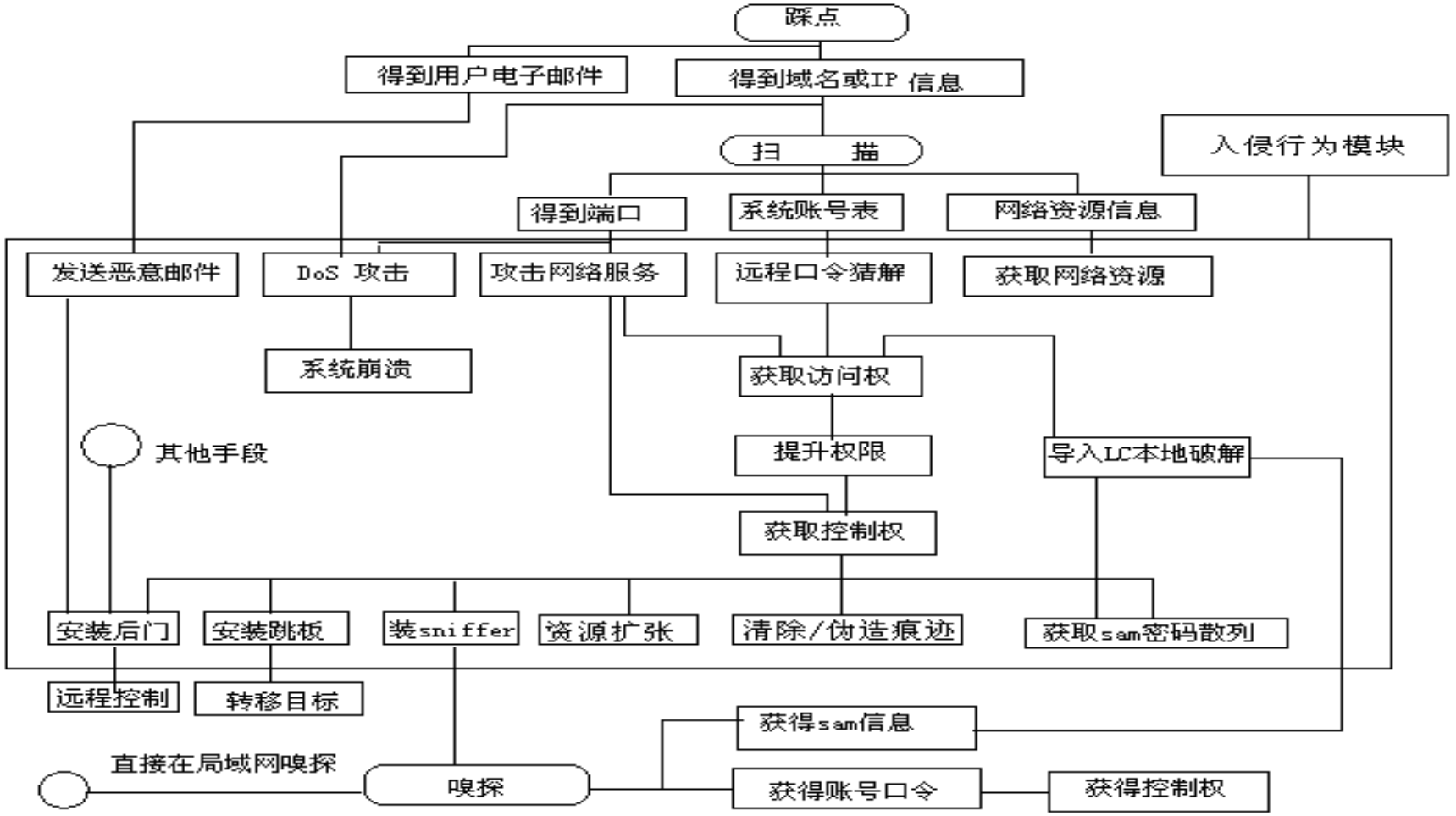
继续渗透网络，直至获取机密数据

↓ 以此主机为跳板，寻找其他主机的漏洞

消灭踪迹 消除所有入侵脚印，以免被管理员发觉

§8.1 黑客概述

- 黑客入侵的行为模型



§8.1 黑客概述

- 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
  - 利用电话交换技术先通过拨号找寻并连入某台主机，然后通过这台主机再连入因特网来跳跃
- 踩点

大多数的DNS服务器允许用户获取域名记录文件内容，这样就可以了解到网站的详细网络分布结构。另外网络服务商可以查询得到公司地址及人员内容邮件、电话等，及单位注册的IP范围等重要信息。

§8.1 黑客概述

- 资源扩张

  指利用已经获得的密码尝试登录其他主机或者其他服务。

- 其他手段

  指类似于发送恶意电子邮件的方式，比如通过恶意网页等其他欺骗方式。还包括近来一些利用Win NT或Windows 2000会话缺陷在远程嗅探其密码的新攻击方法。

§8.1 黑客概述

- 预攻击探测
  - Ping扫描：用于发现攻击目标
  - 操作系统识别扫描：对目标主机运行的操作系统进行识别
  - 端口扫描：用于查看攻击目标处于监听或运行状态的服务
  - 漏洞扫描：扫描对方系统有什么漏洞可以利用
- 目前主流的扫描工具包括流光、Nmap、 Nessus、SSS等都实现了这些技术。

§8.1 黑客概述

- 采取攻击行为

在攻击探测中如果攻击者发现目标机器系统有可以被利用的漏洞或弱点，则立即采取攻击行为。在此过程中具体采用的攻击行为要视目标机器系统而定，目前较流行的手段有暴力破解、缓冲区溢出、跨站脚本、拒绝服务、欺骗等。

- 清除痕迹

清除攻击痕迹的方法主要是清除系统和服务日志。有些工具可以清除日志，如THC提供的cleara.c。

在Windows操作系统里面主要是清除C:\Windows\system32\config目录下的log文件。

§8.2 网络扫描

- 扫描器是自动检测远程或本地主机安全性漏洞的程序包。
- 使用扫描器，不仅可以很快地发现本地主机系统配置和软件上存在的安全隐患，而且还可以不留痕迹地发现远在另一个半球的一台主机的安全性漏洞，这种自动检测功能快速而准确。
- 不同的人使用扫描器会有不同的结果：如果系统管理员使用了扫描器，它将直接有助于加强系统安全性；而对于黑客来说，扫描器是他们进行攻击入手点，不过，由于扫描器不能直接攻击网络漏洞，所以黑客使用扫描器找出目标主机上各种各样的安全漏洞后，利用其他方法进行恶意攻击。

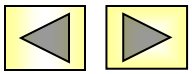
§8.2 网络扫描



- 操作系统本身的ping工具

```
C:\>ping 10.1.1.2
Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Ping statistics for 10.1.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

TTL=125左右的主机应该是Windows系列的

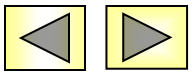


§8.2 网络扫描

- 操作系统本身的ping工具

```
C:\>ping 10.1.1.6
Pinging 10.1.1.6 with 32 bytes of data:
Request timed out.
Reply from 10.1.1.6: bytes=32 time=250ms TTL=237
Reply from 10.1.1.6: bytes=32 time=234ms TTL=237
Reply from 10.1.1.6: bytes=32 time=234ms TTL=237
Ping statistics for 10.1.1.6:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 234ms, Maximum = 250ms, Average = 179ms
```

TTL=235左右的主机应该是Unix系列的



§ 8.2 网络扫描

- 主机扫描——工具软件：SuperScan

主界面



§ 8.2 网络扫描

- 主机扫描——工具软件：SuperScan



§8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser

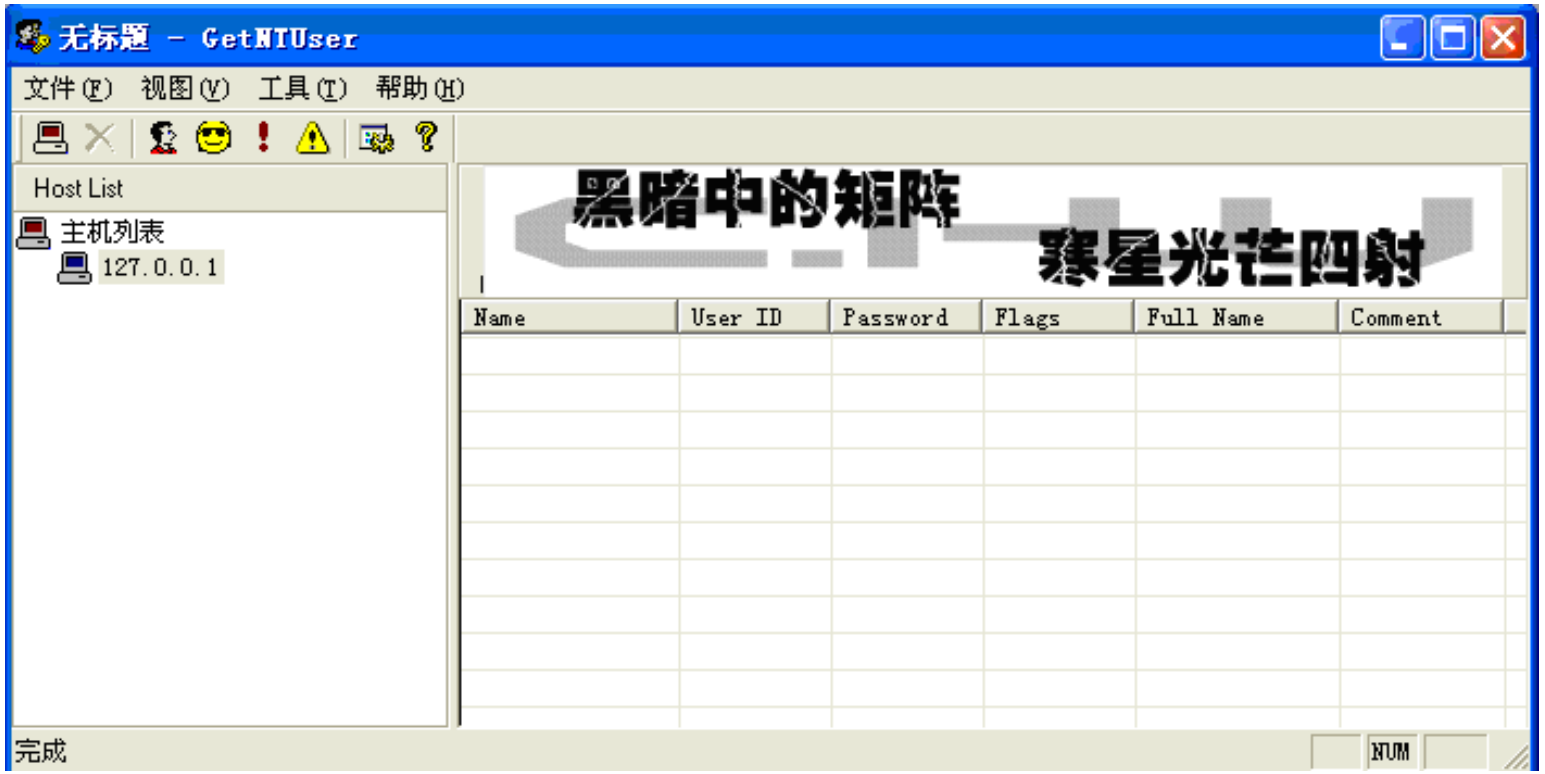
主要功能：

- 扫描出NT主机上存在的用户名。
- 自动猜测空密码和与用户名相同的密码。
- 可以使用指定密码字典猜测密码。
- 可以使用指定字符来穷举猜测密码。

§ 8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser

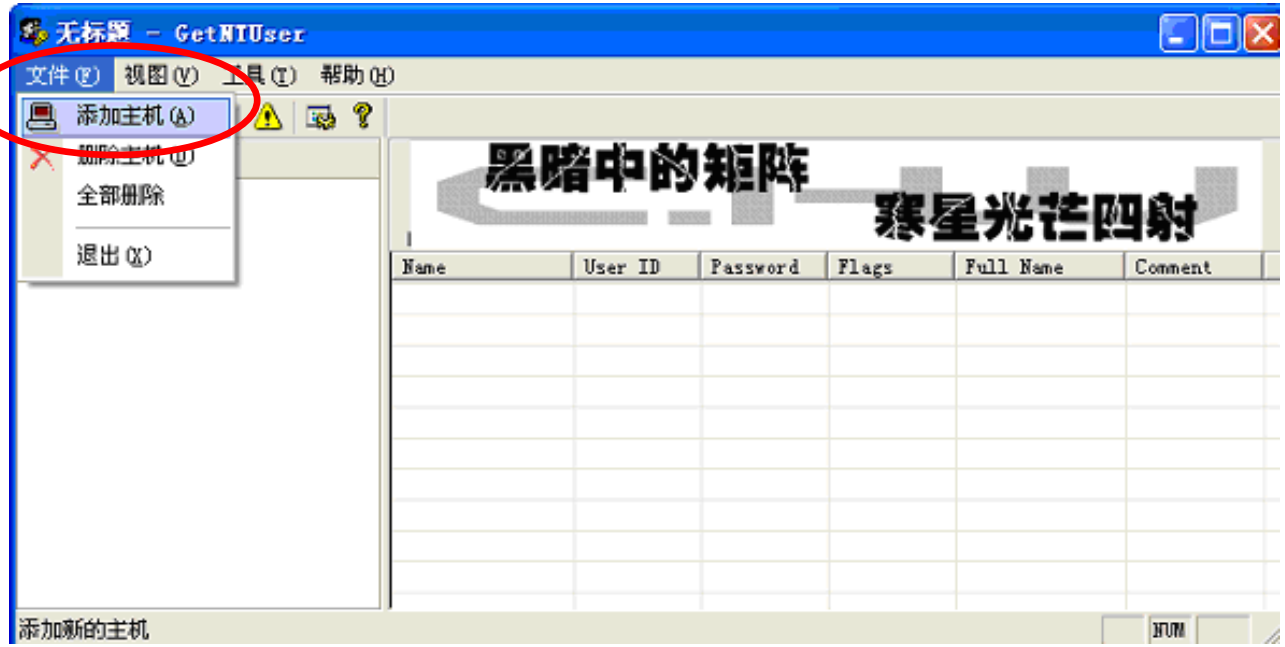
主界面

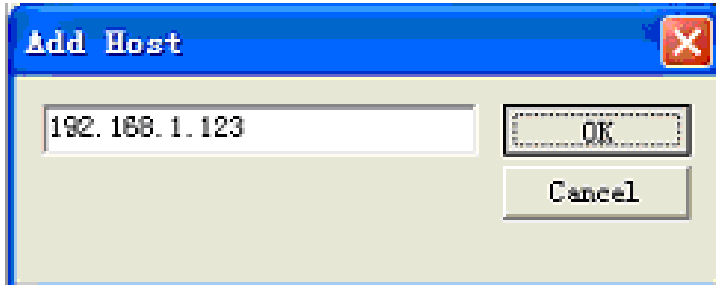


§ 8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser

设置扫描的目标主机

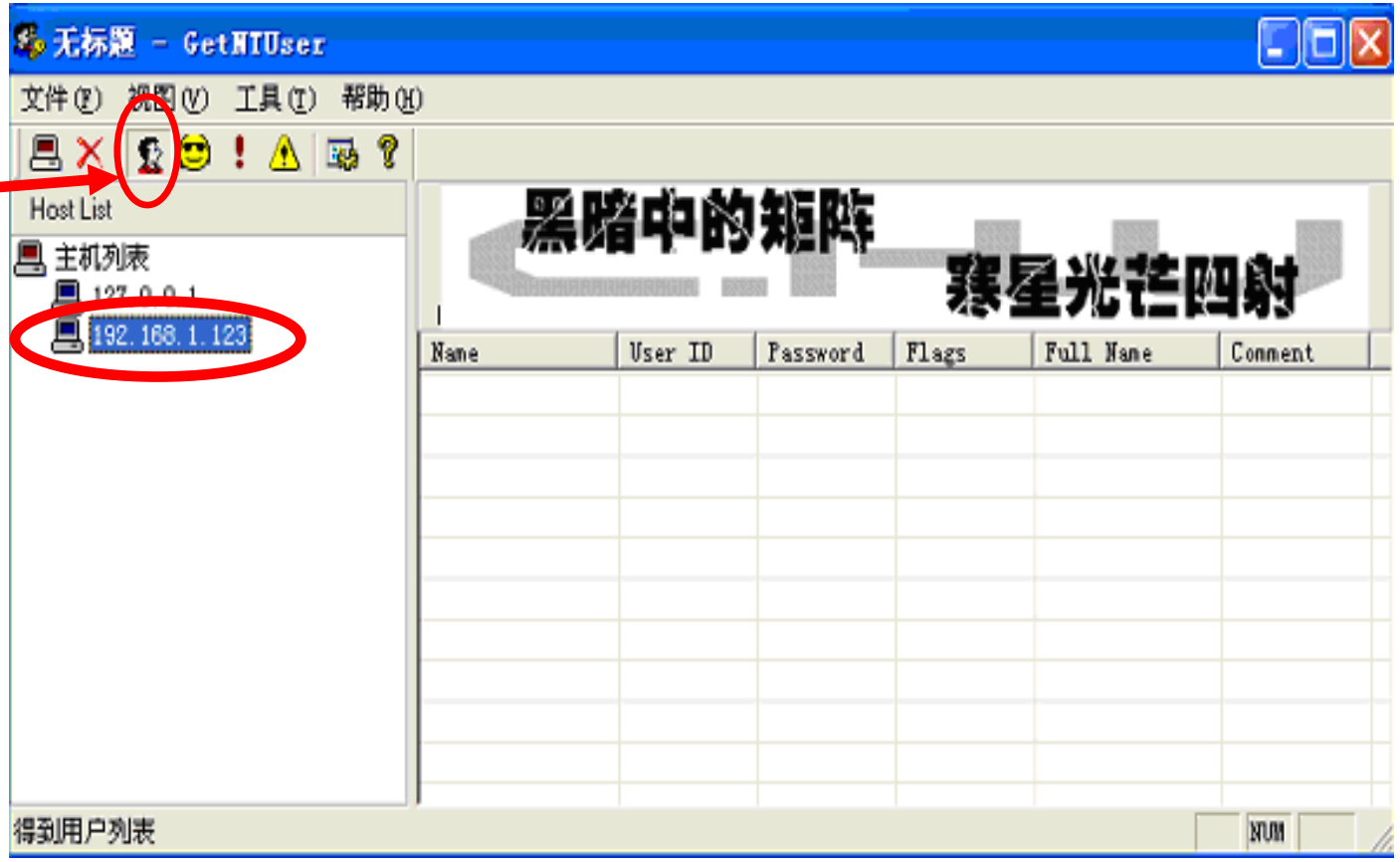




§ 8.2 网络扫描

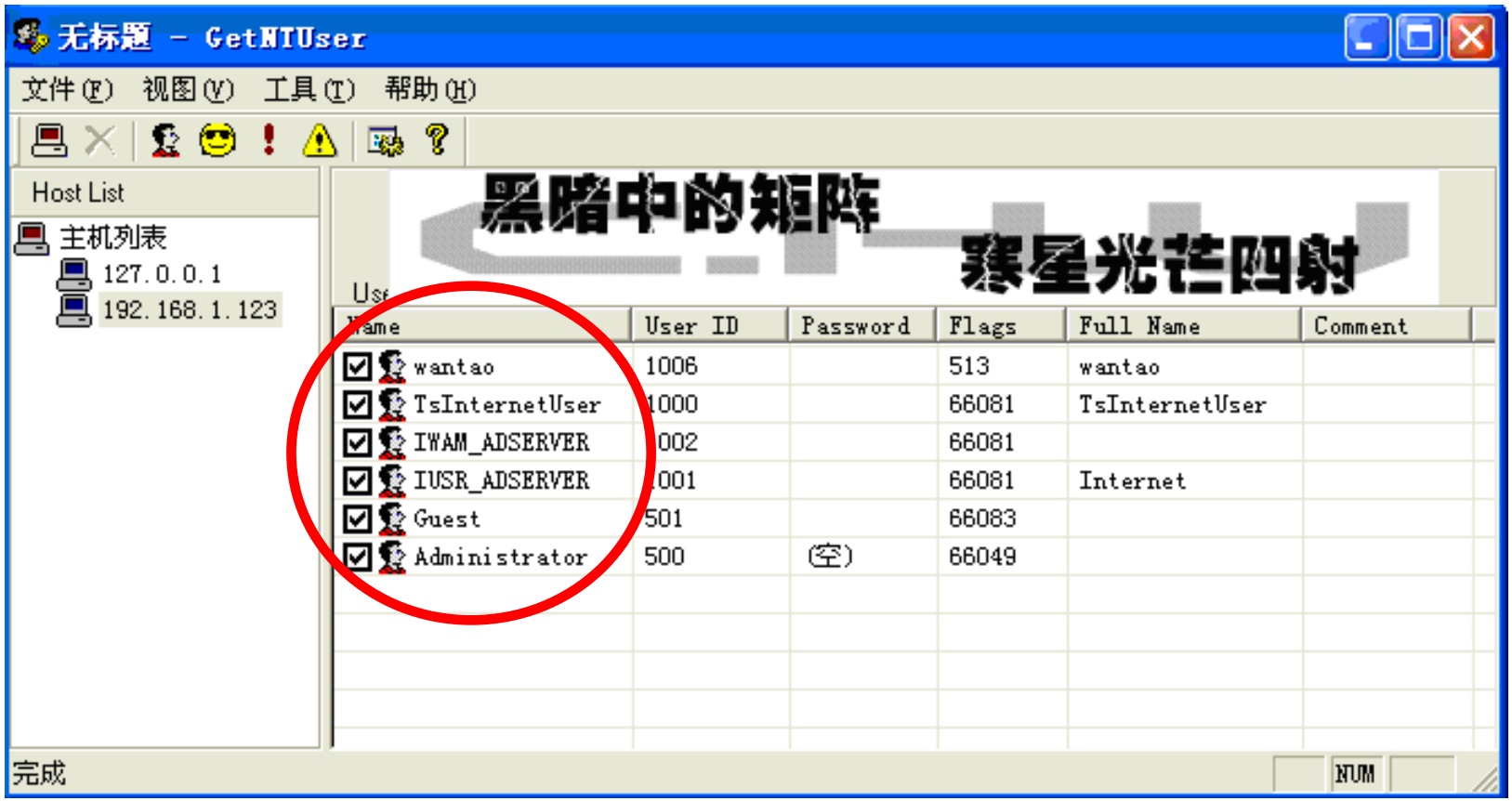
- 系统用户扫描——工具软件：GetNTUser

获得用户列表



§8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser



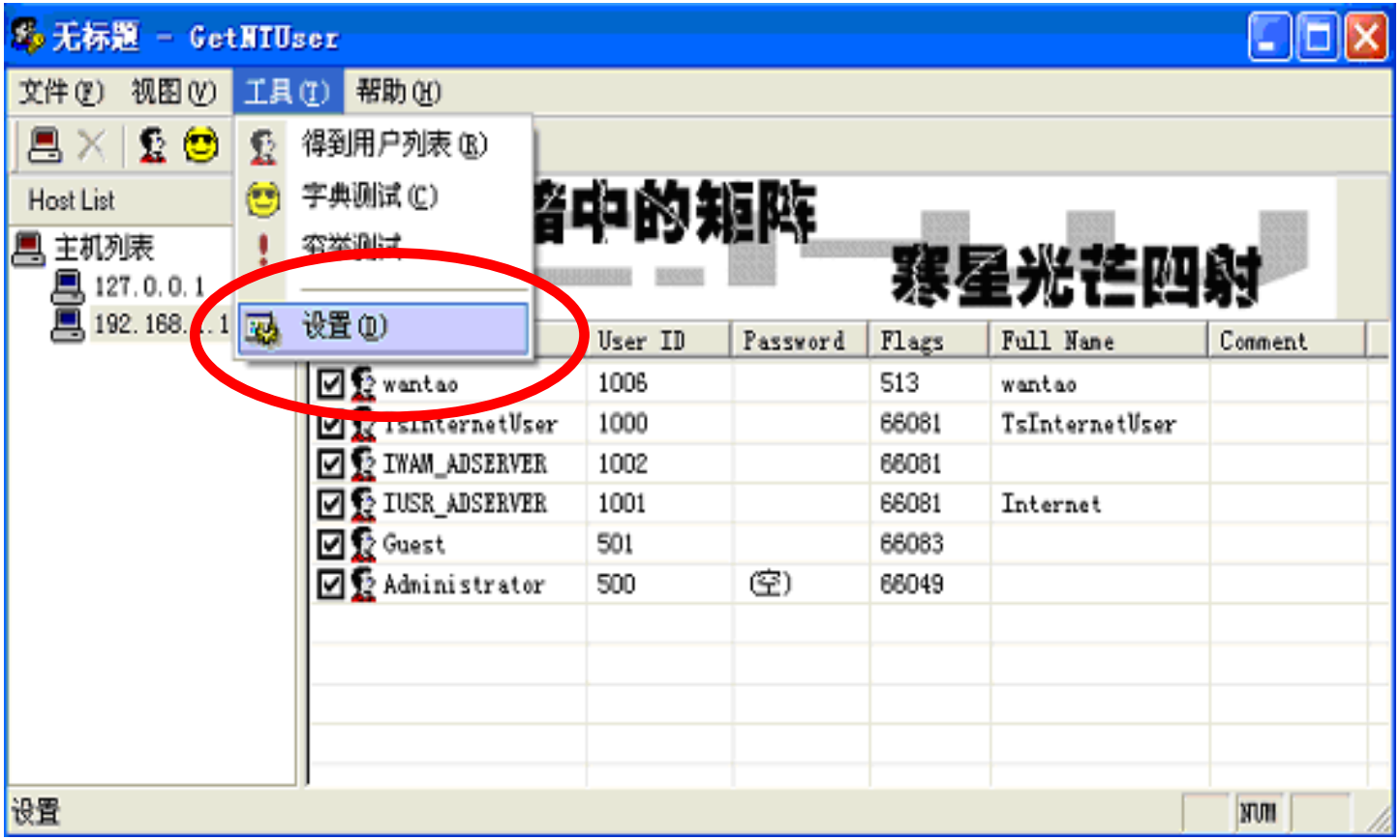
§8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser

设置

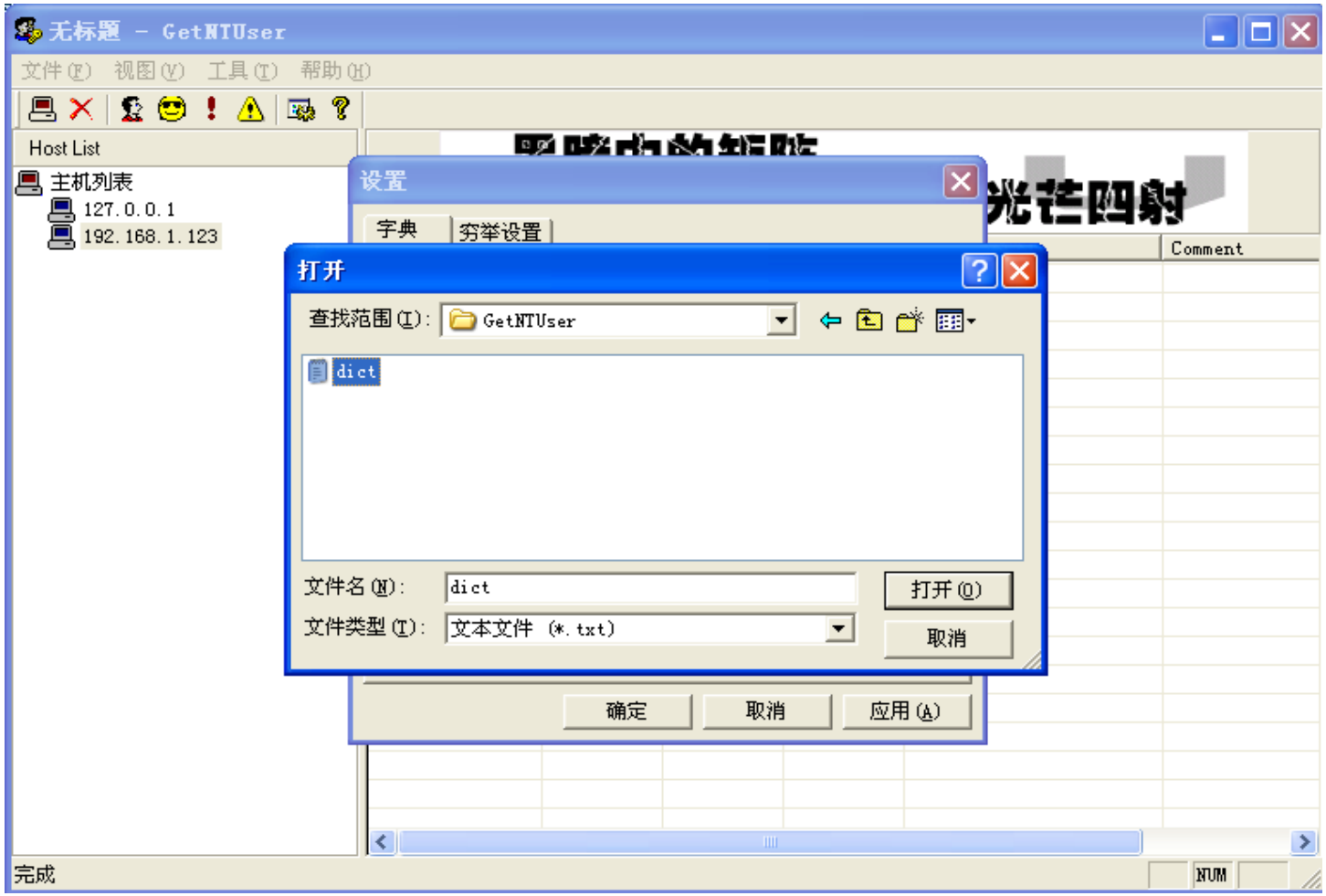
字典

文件



§ 8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser



§8.2 网络扫描

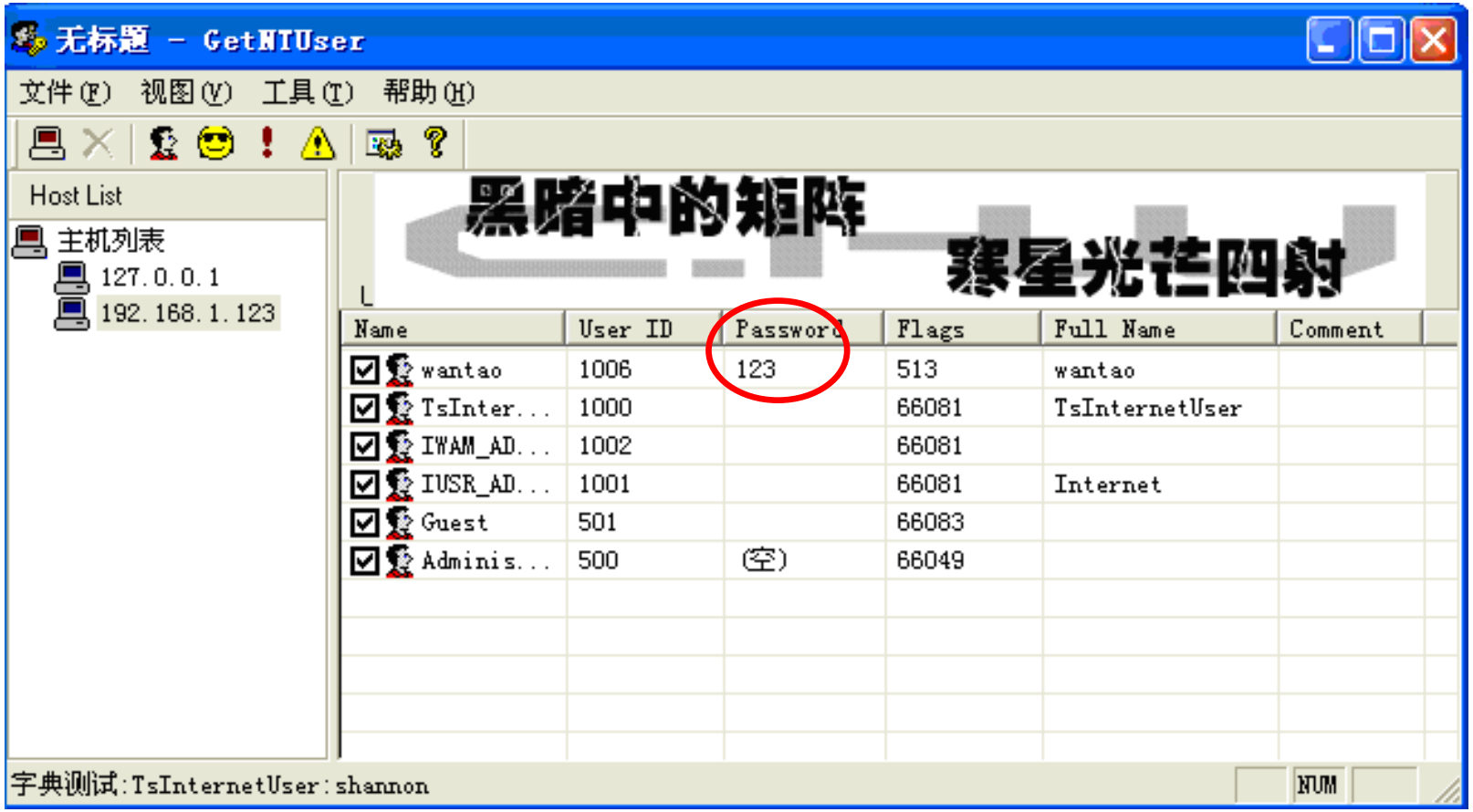
- 系统用户扫描——工具软件：GetNTUser

使用字典文件对用户口令进行测试



§8.2 网络扫描

- 系统用户扫描——工具软件：GetNTUser



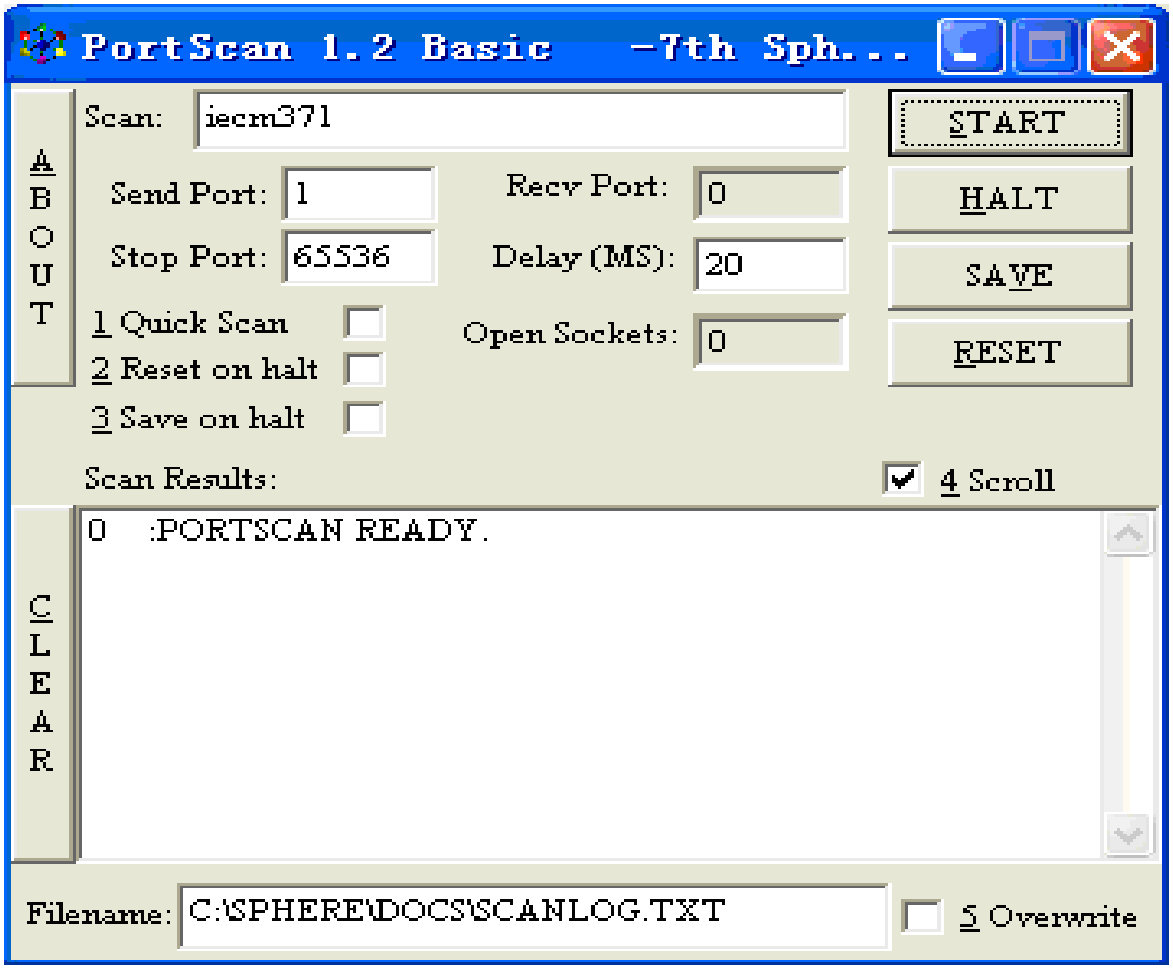
§8.2 网络扫描

- 端口扫描工具
  - PortScan
  - SuperScan
  - NetScanTools
  - WinScan
  - NTOScanner
  - WUPS
  - NmapNT

§ 8.2 网络扫描

- 开放端口扫描——工具软件：PortScan

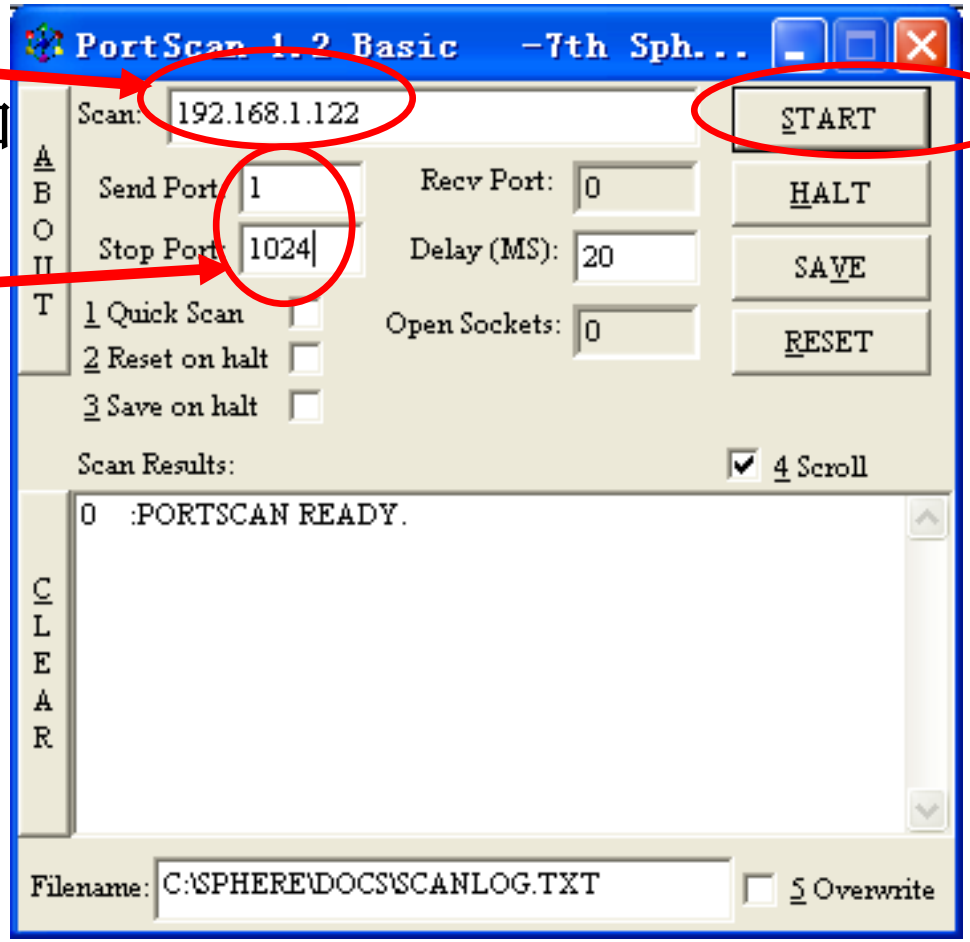
主界面



§ 8.2 网络扫描

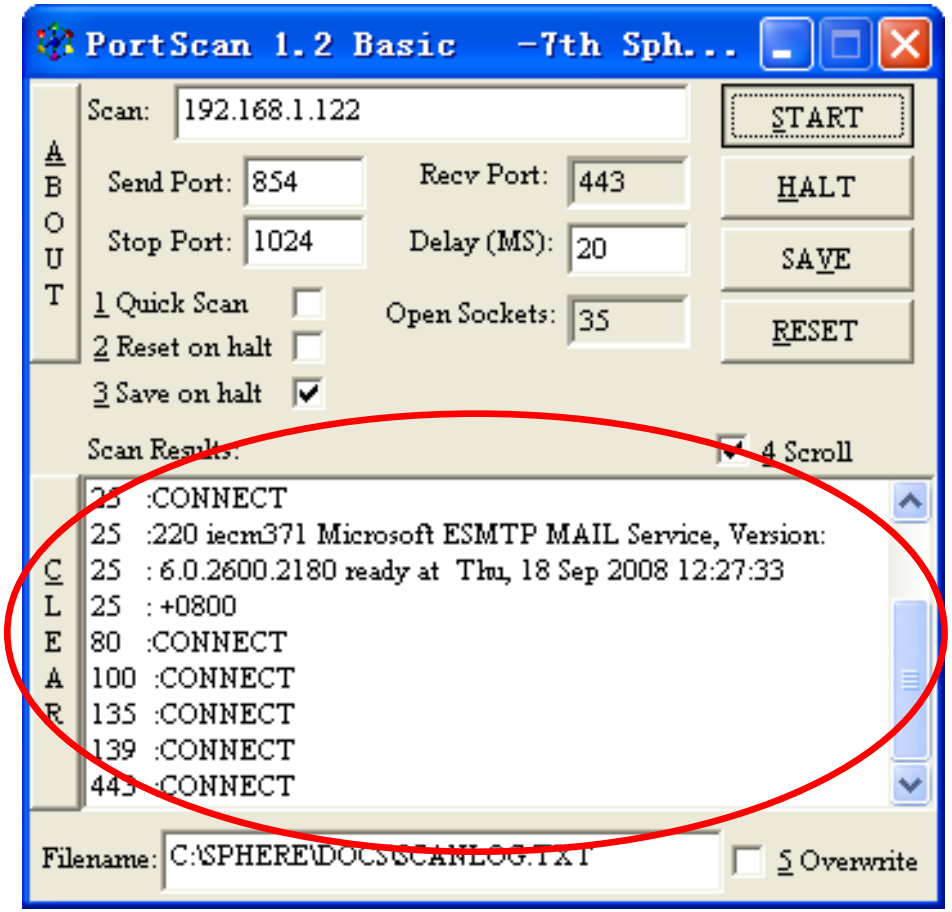
- 开放端口扫描——工具软件：PortScan

设置目标主机和端口范围后单击Start



§ 8.2 网络扫描

- 开放端口扫描——工具软件：PortScan



§8.2 网络扫描

- 开放端口扫描——工具软件：SuperScan

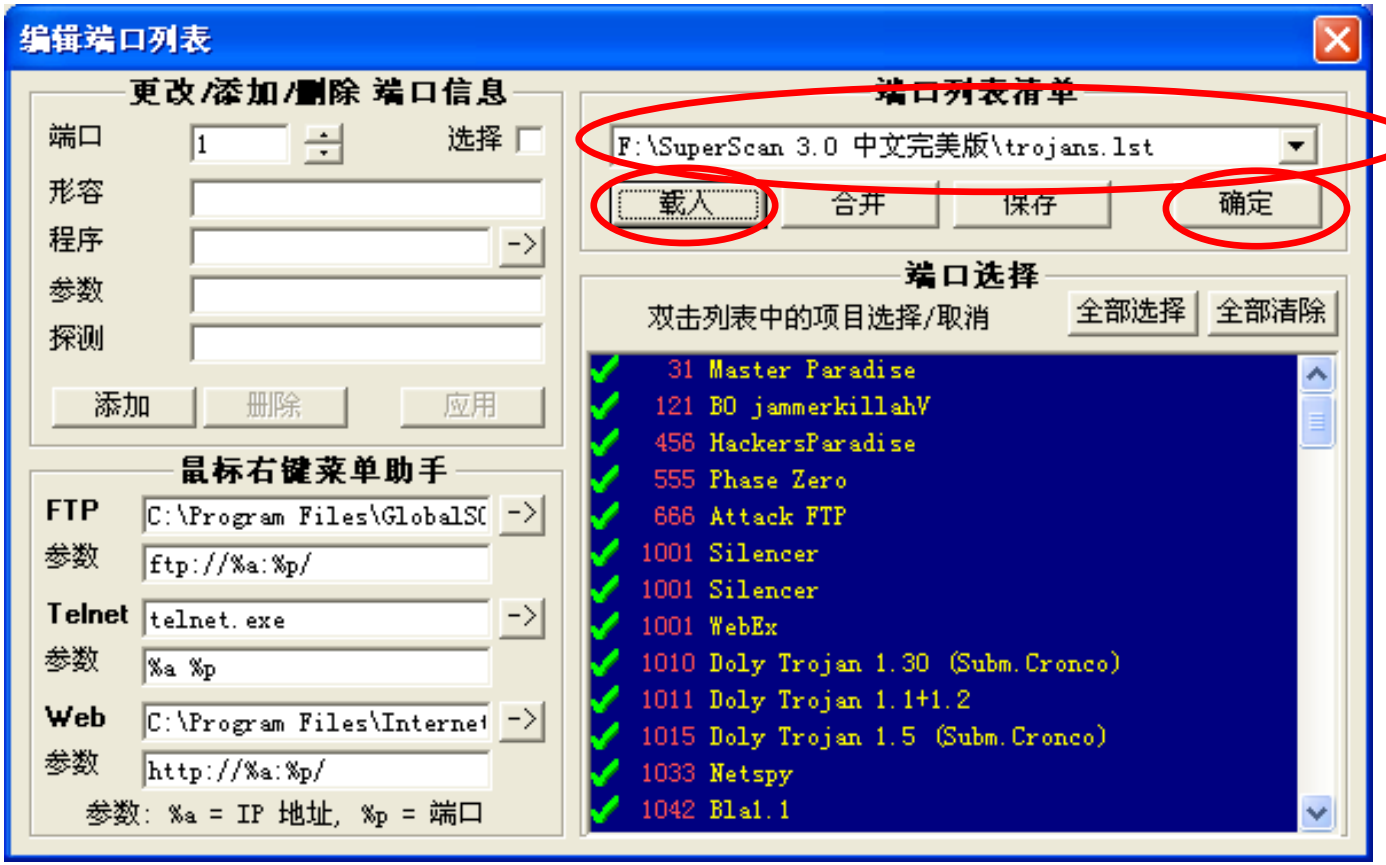
主界面



§ 8.2 网络扫描

- 开放端口扫描——工具软件：SuperScan

端口扫描



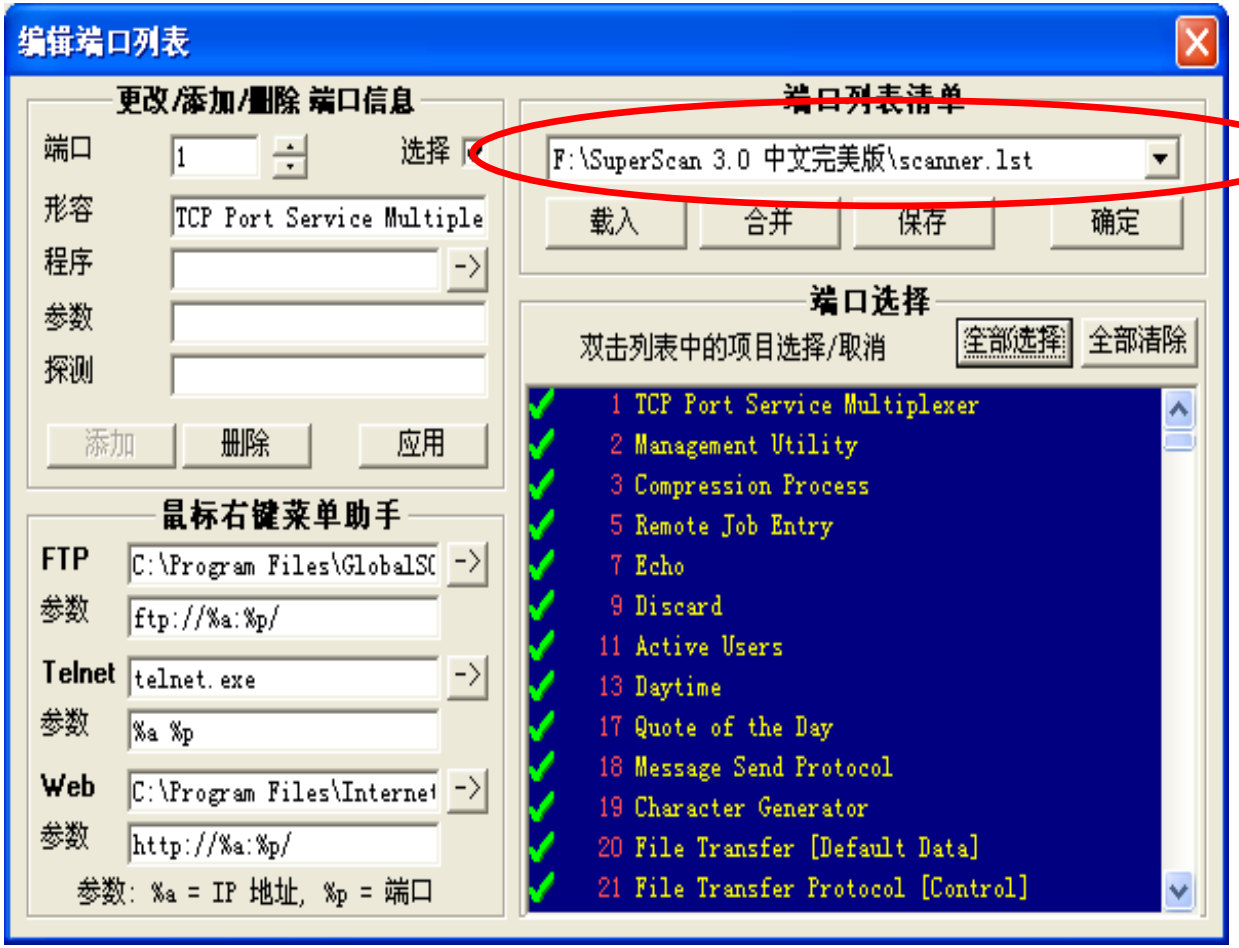
§ 8.2 网络扫描

- 开放端口扫描——工具软件：SuperScan



§8.2 网络扫描

- 开放端口扫描——工具软件：SuperScan



§ 8.2 网络扫描

- 开放端口扫描——工具软件：SuperScan



§8.2 网络扫描

- 共享目录扫描——工具软件：Shed

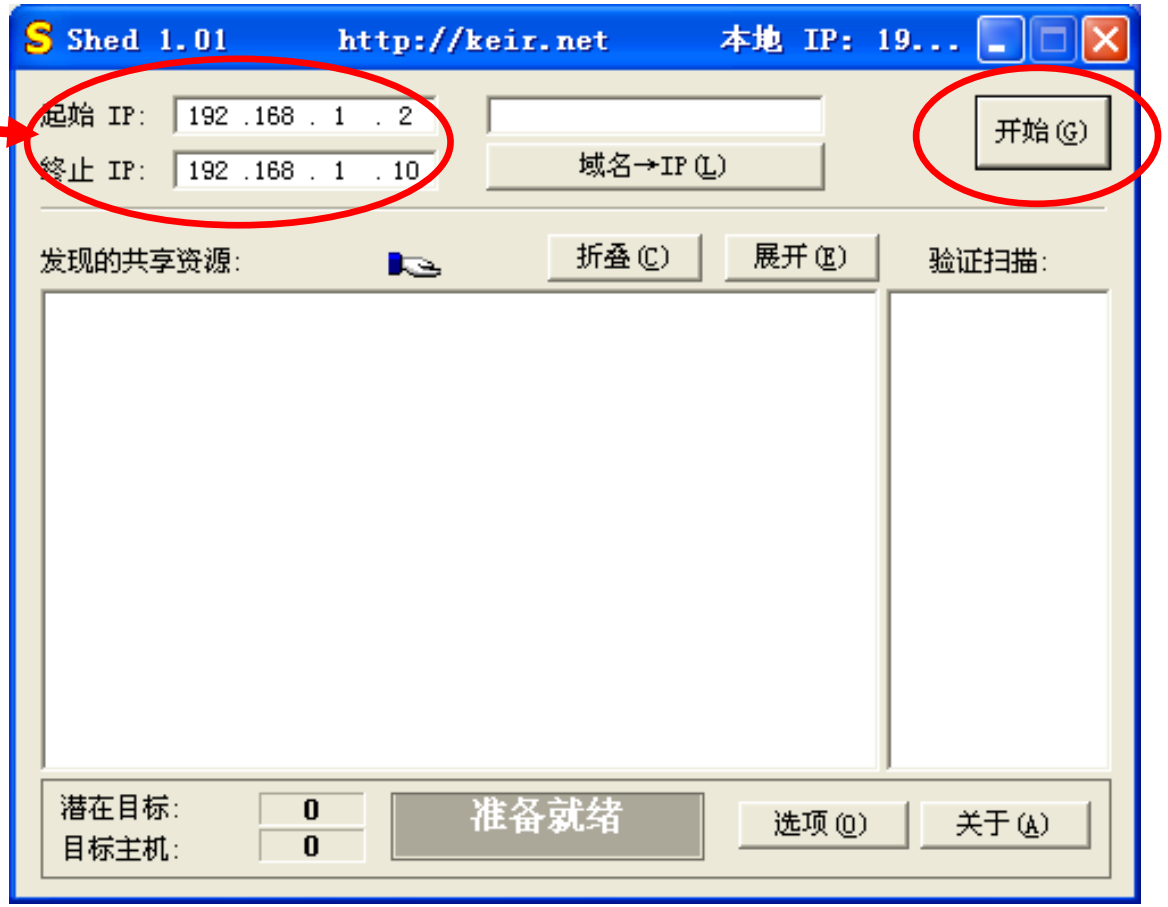
主界面



§ 8.2 网络扫描

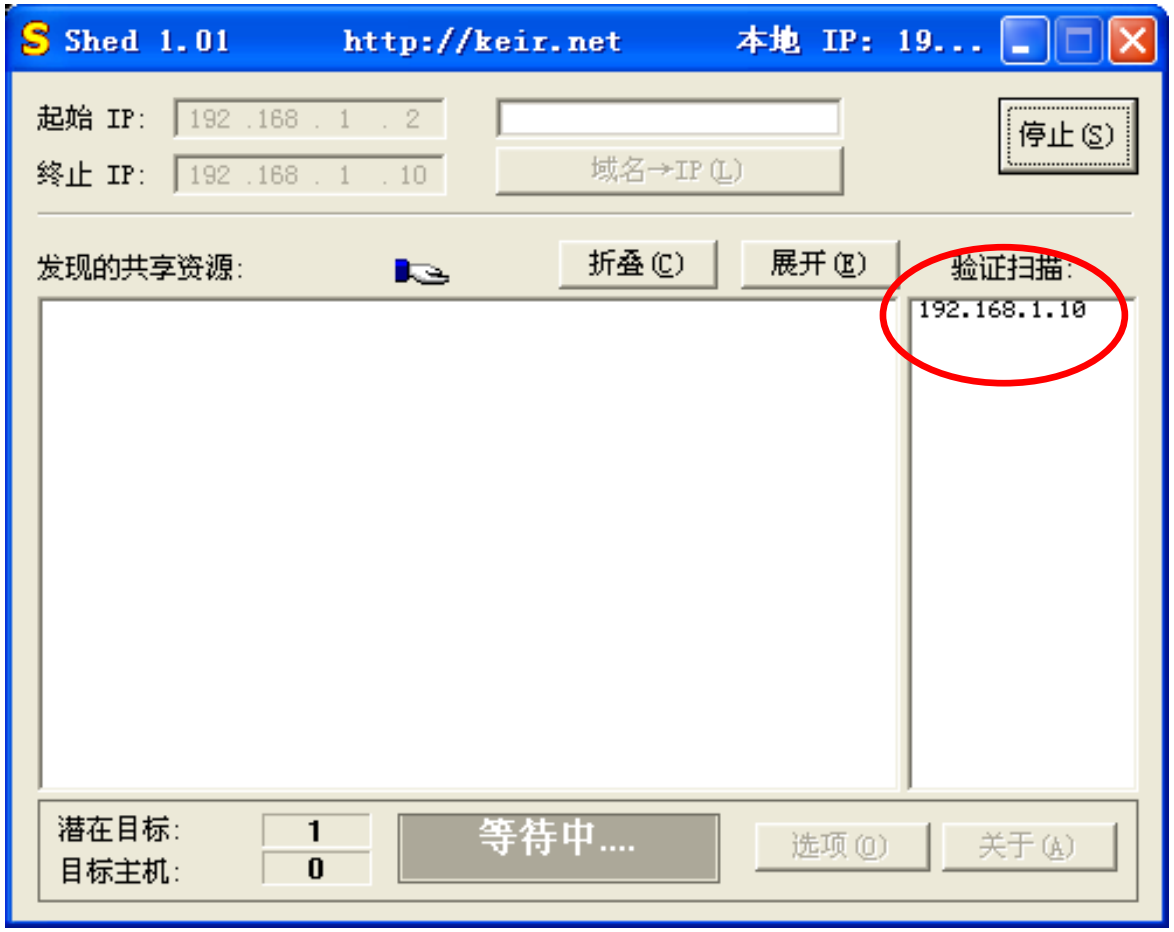
- 共享目录扫描——工具软件：Shed

设置扫描的主机范围



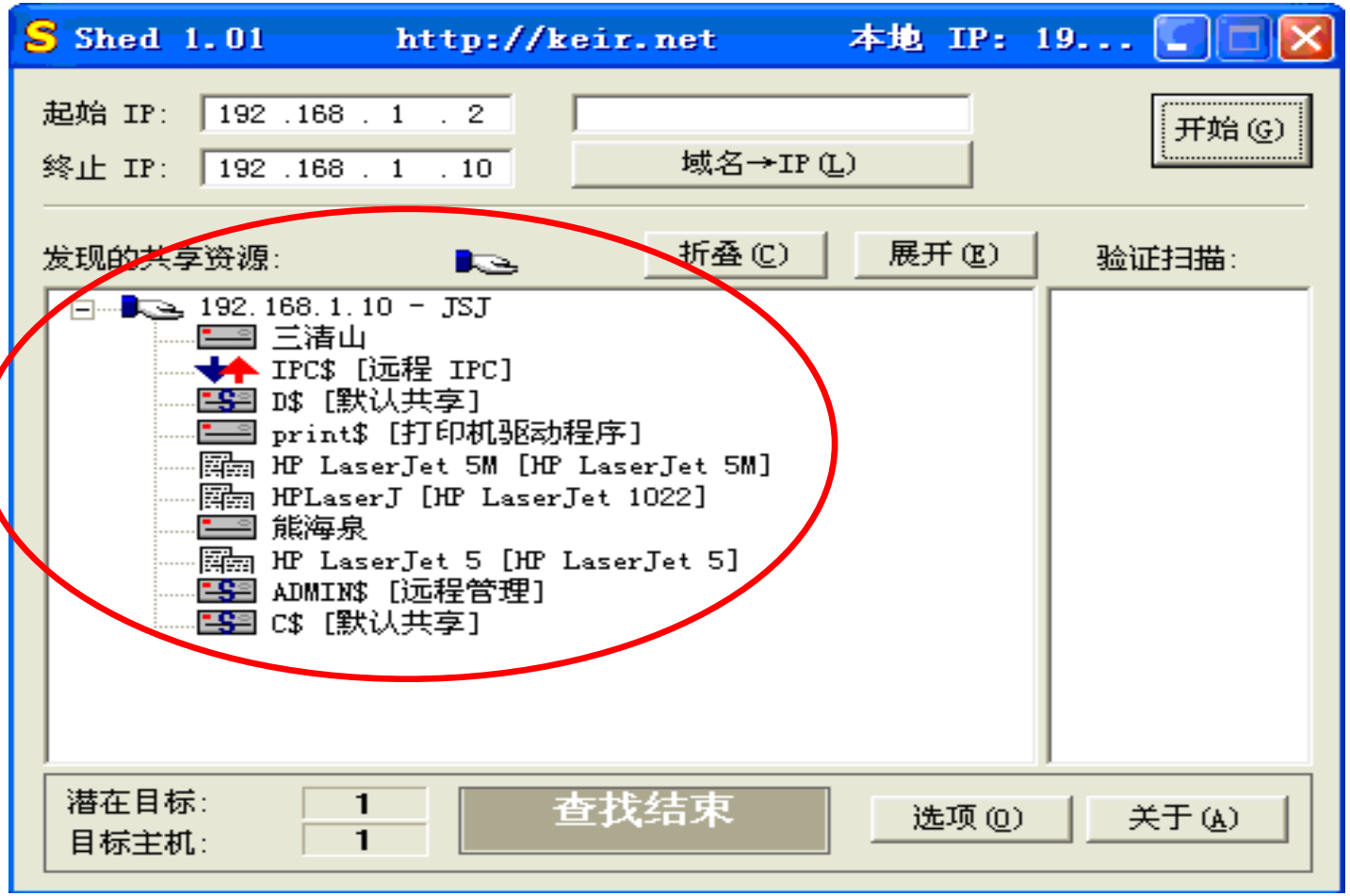
§8.2 网络扫描

- 共享目录扫描——工具软件：Shed



§ 8.2 网络扫描

- 共享目录扫描——工具软件：Shed



§8.2 网络扫描

- 针对预攻击探测的防范措施
  - Ping sweep：安装防火墙或相关工具软件，禁止某些ICMP ping，使用NAT隐藏内部网络结构
  - Port scan：安装防火墙或相关工具软件，禁止访问不该访问的服务端口
  - OS fingerprint：安装防火墙或相关工具软件，只允许访问少量服务端口，缺乏必要的信息，无法判断OS类型
  - 资源和用户扫描：防范NetBIOS扫描的最直接方法就是不允许对TCP/UDP 135到139端口的访问，如通过防火墙或路由器的配置等。对单独的主机，可使用NetBIOS over TCP/IP项失效或注册表配置来实现。

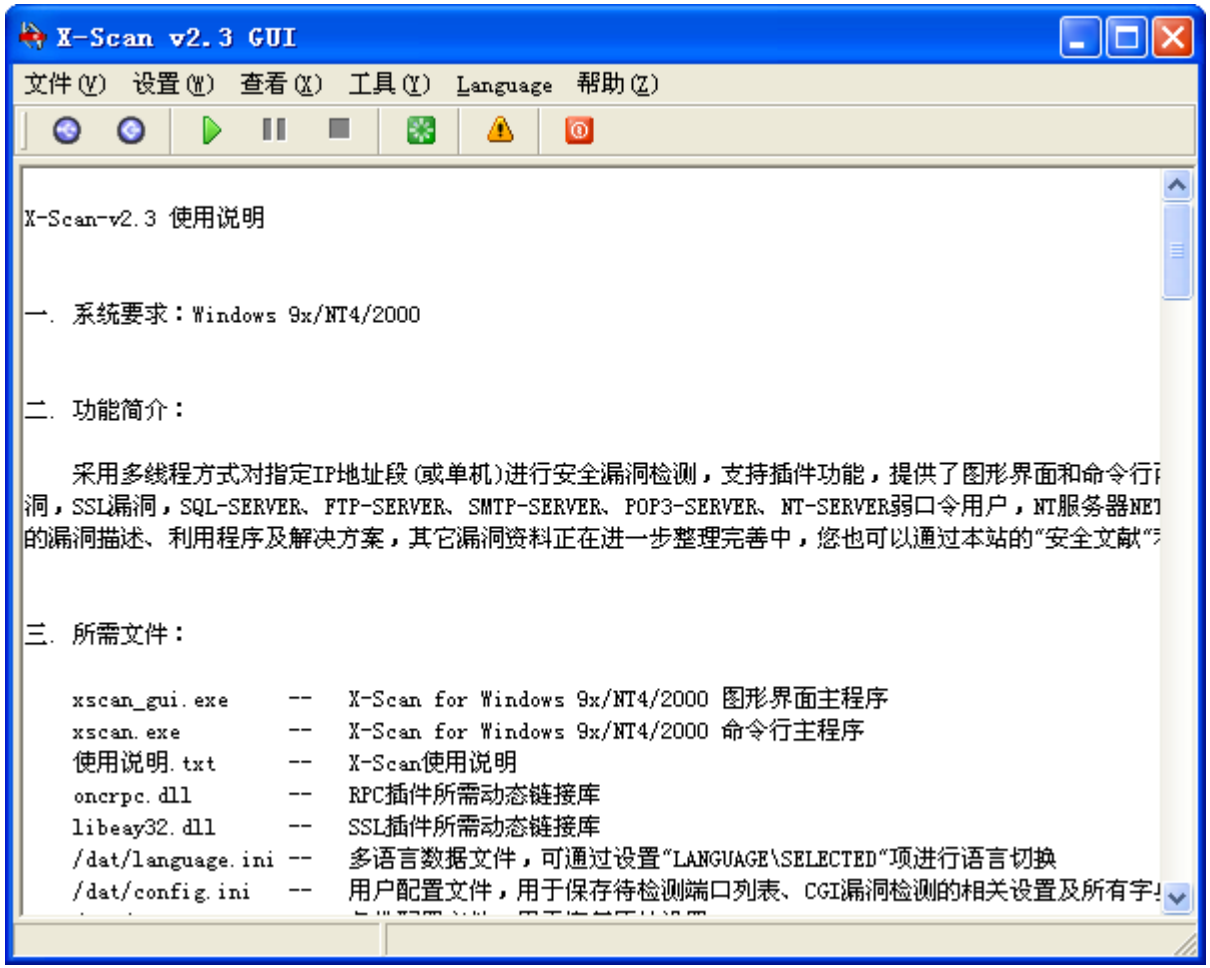
§8.2 网络扫描

- 漏洞扫描
  - 漏洞扫描是一种最常见的攻击模式，用于探测系统和网络漏洞，如获取系统和应用口令，嗅探敏感信息，利用缓存区溢出直接攻击等。
  - 针对某一类型的漏洞，都有专门的攻击工具。也有一些功能强大综合扫描工具，对系统进行全面探测和漏洞扫描。
- 综合漏洞扫描和攻击工具
  - X-Scan
  - 流光
  - SSS

§ 8.2 网络扫描

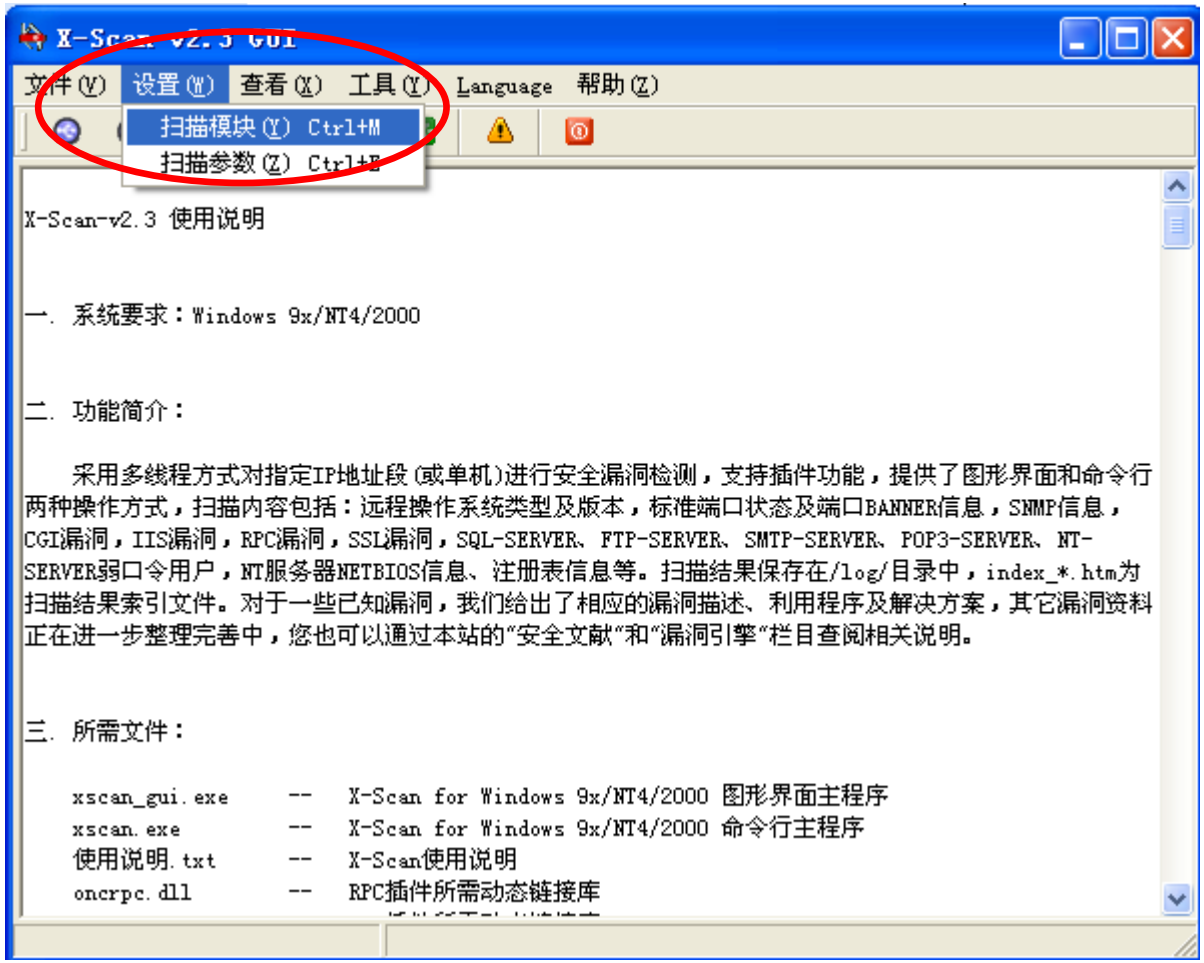
- 漏洞扫描——工具软件：X-Scan

主界面



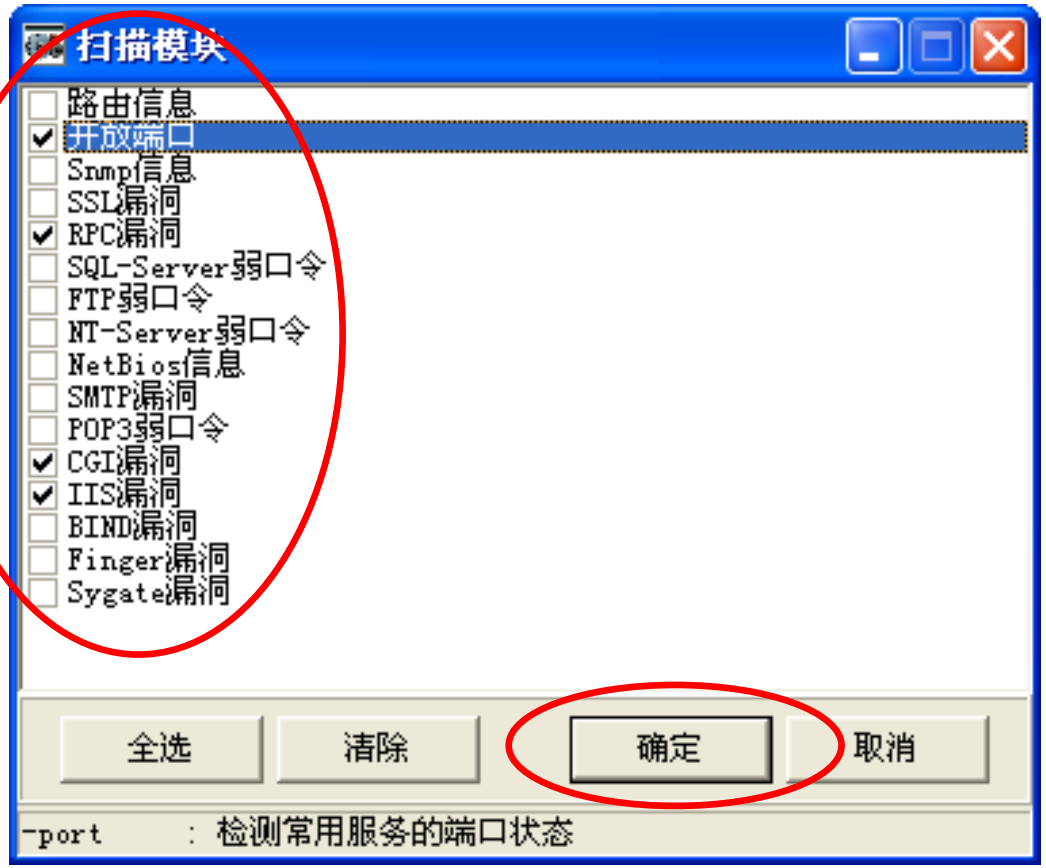
§ 8.2 网络扫描

- 漏洞扫描——工具软件：X-Scan



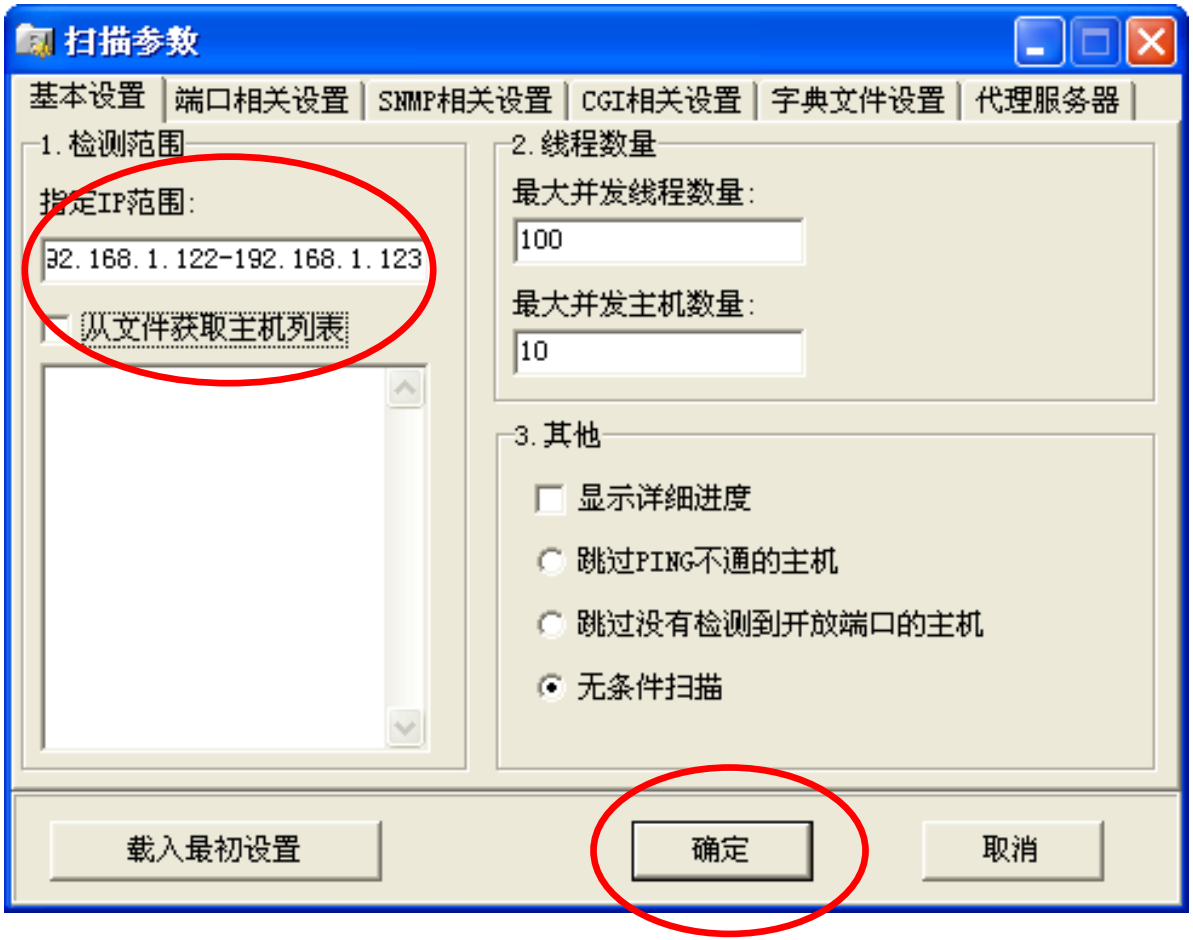
§8.2 网络扫描

- 漏洞扫描——工具软件：X-Scan



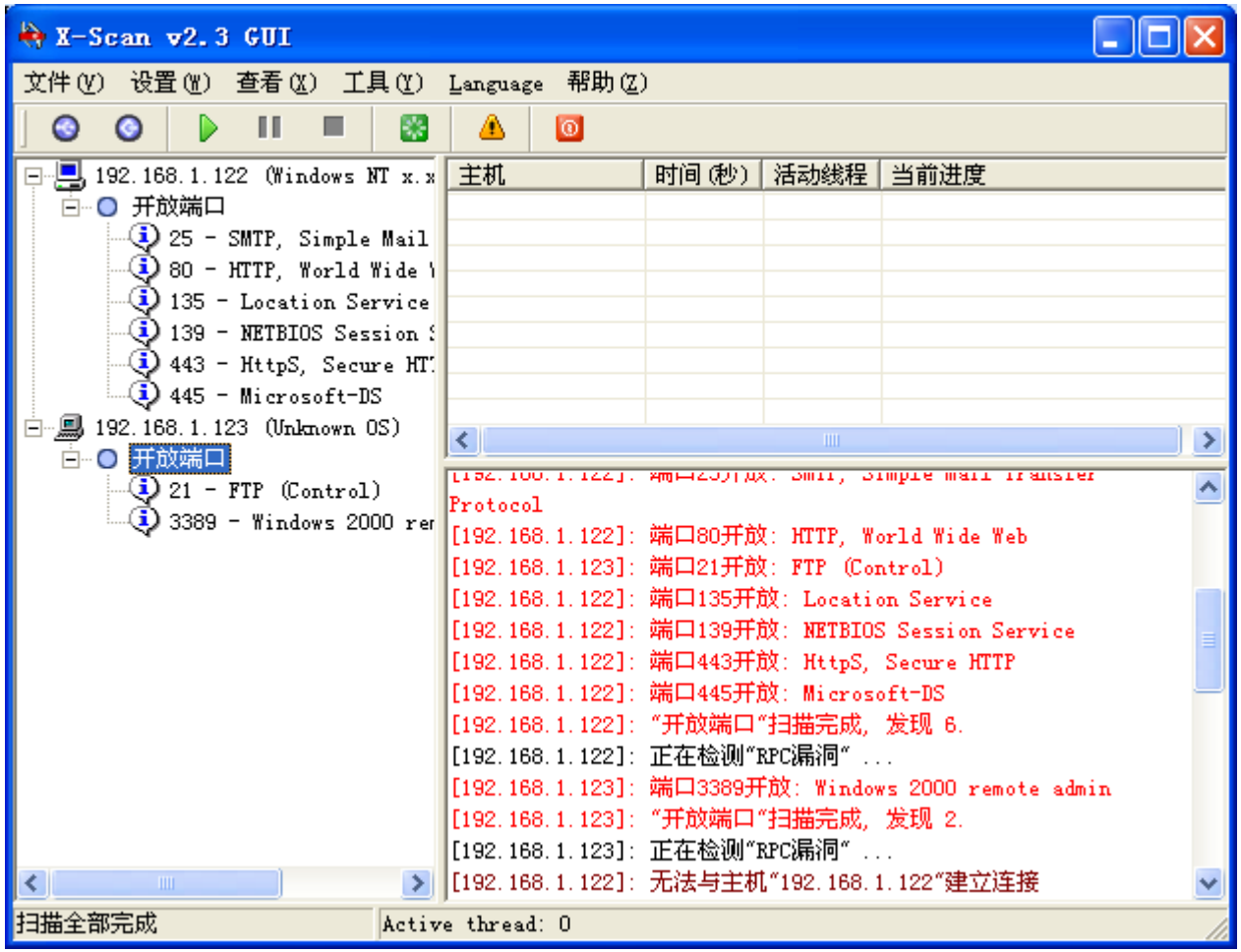
§8.2 网络扫描

- 漏洞扫描——工具软件：X-Scan



§ 8.2 网络扫描

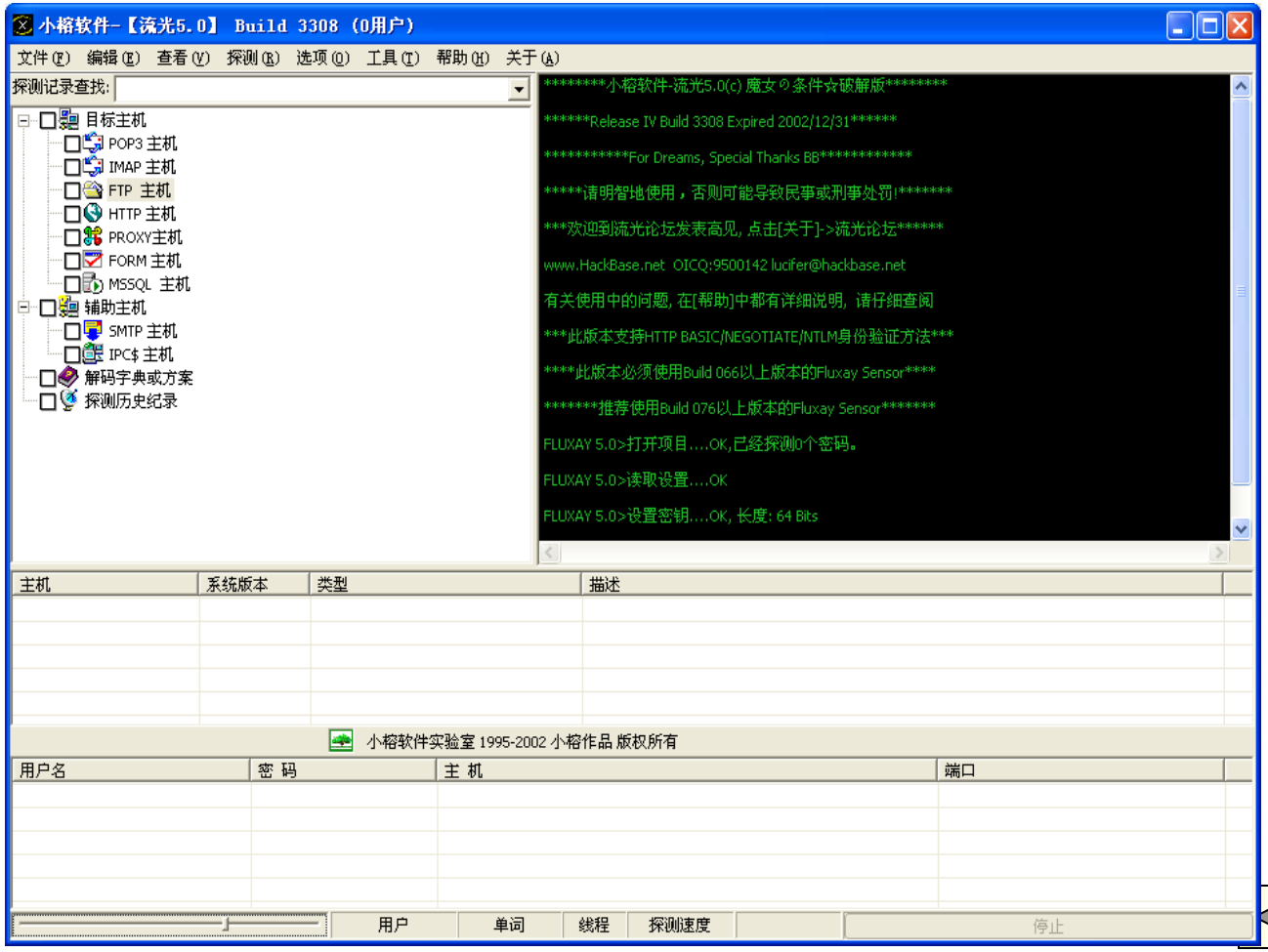
- 漏洞扫描——工具软件：X-Scan



§ 8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay

主界面



§ 8.2 网络扫描

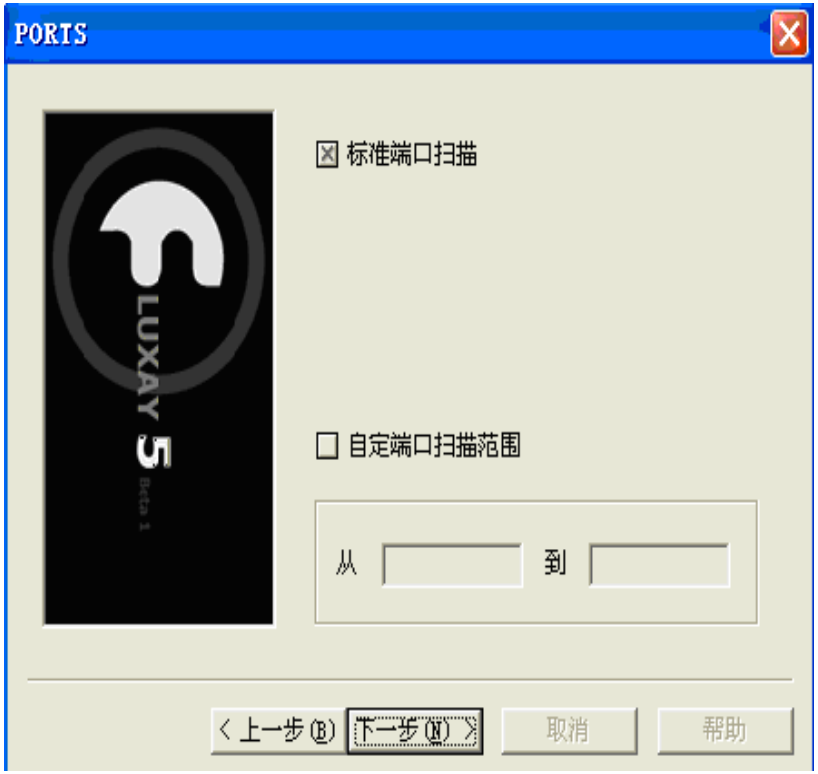
- 漏洞扫描——工具软件：Fluxay



§8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay





§8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay





§8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay





§8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay





§ 8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay





§8.2 网络扫描

- 漏洞扫描——工具软件：Fluxay

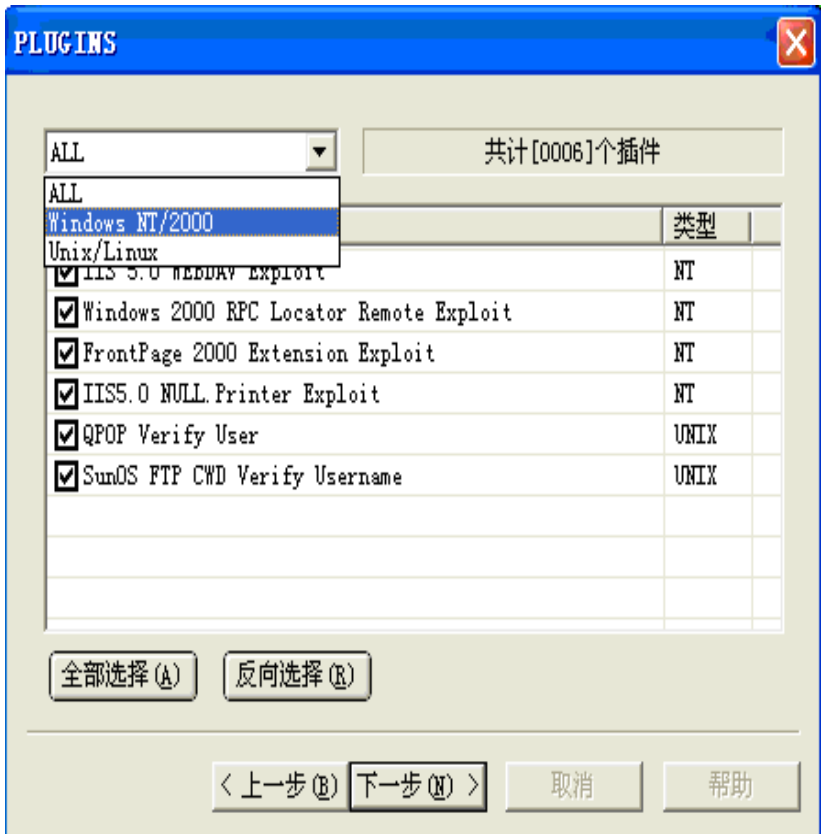




§8.2 网络扫描

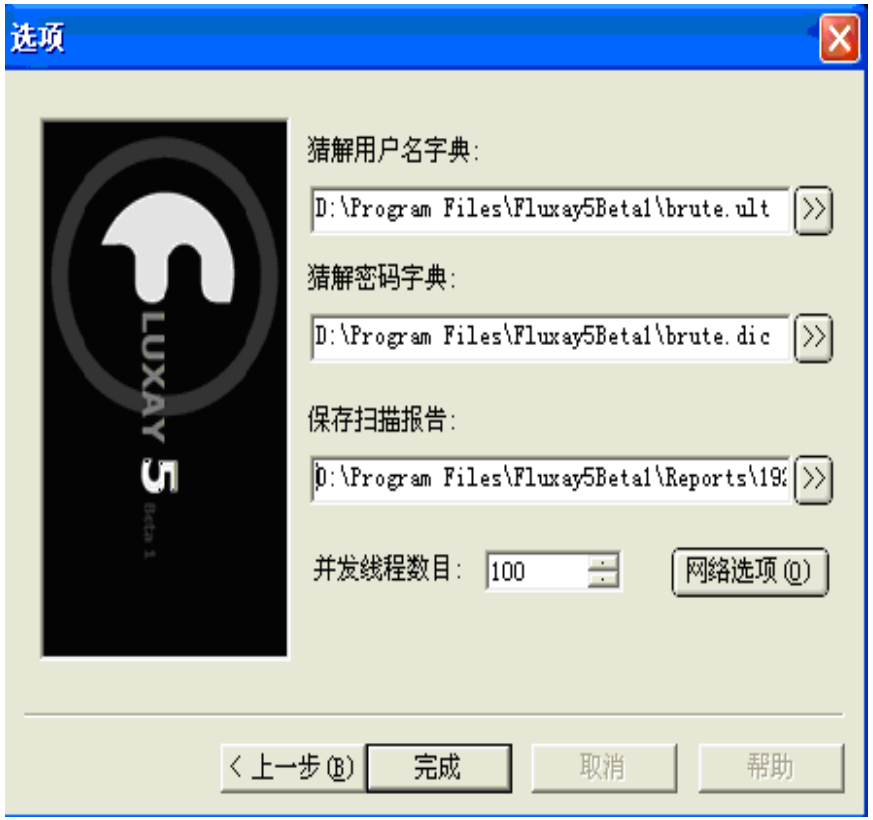
- 漏洞扫描——工具软件：Fluxay

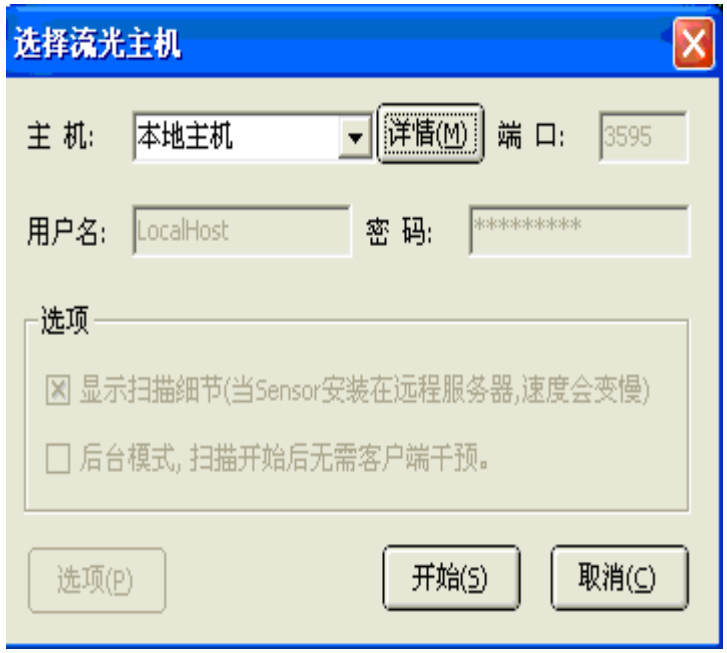




§ 8.2 网络扫描

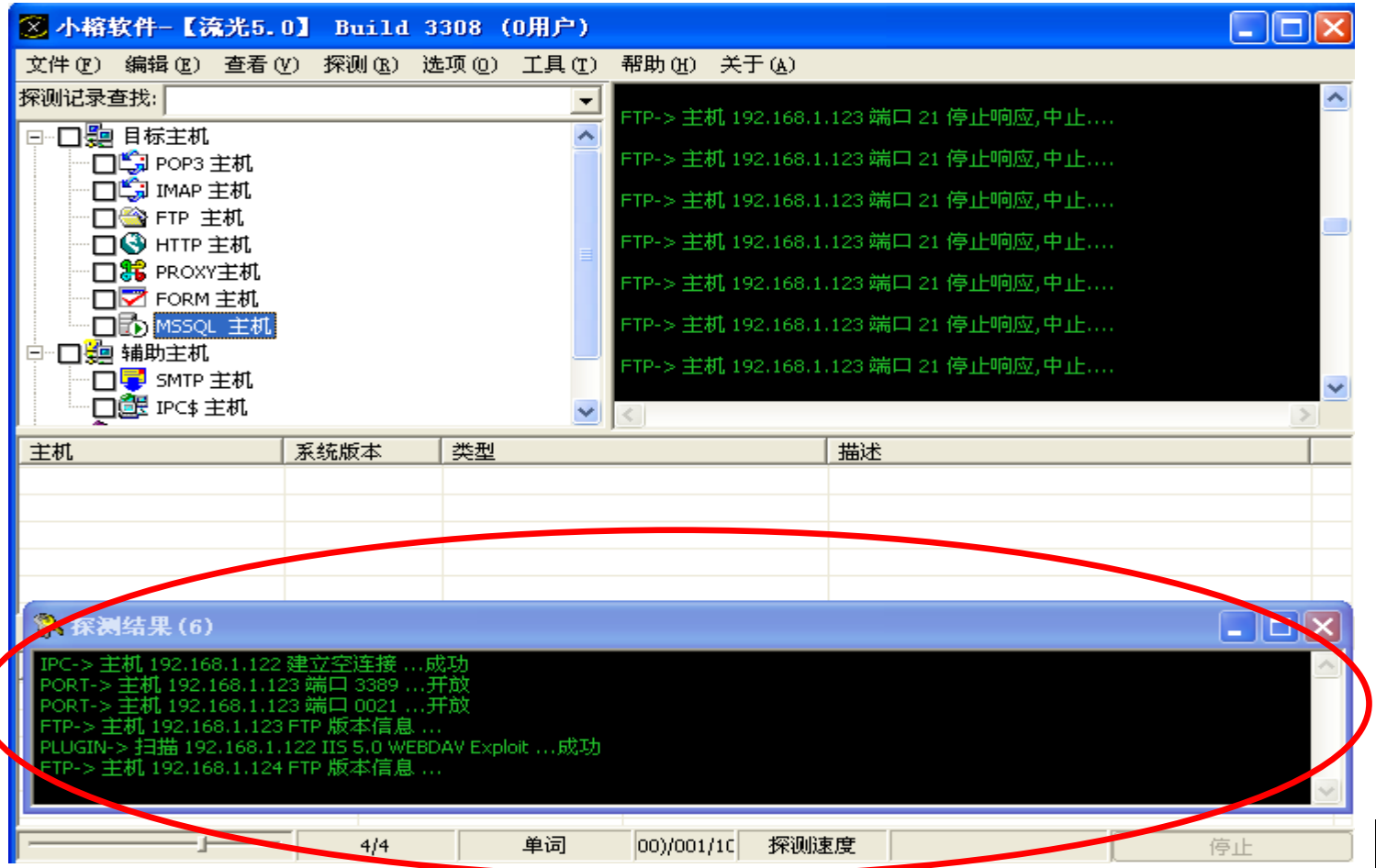
- 漏洞扫描——工具软件：Fluxay





§ 8.2 网络扫描

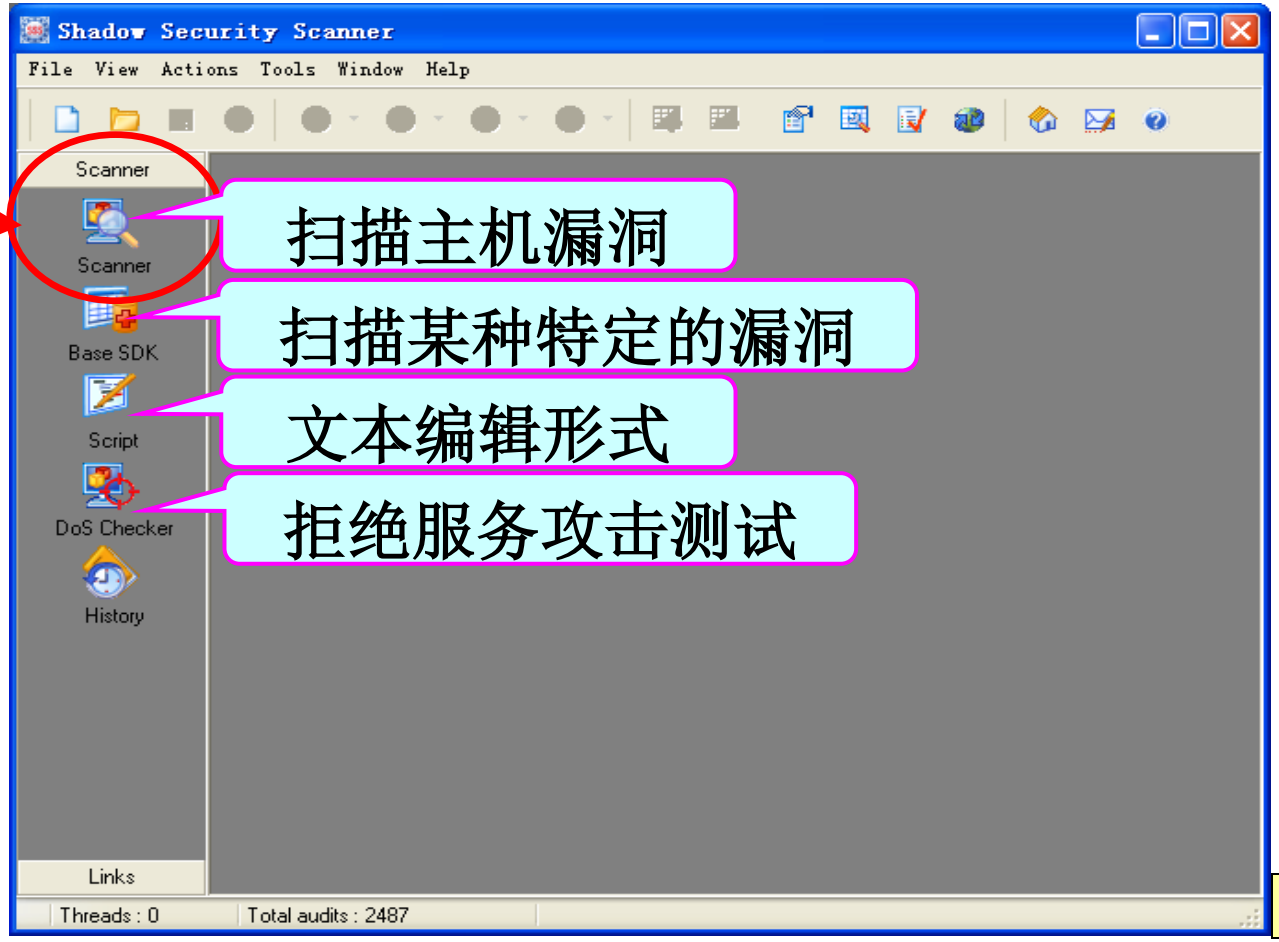
- 漏洞扫描——工具软件：Fluxay



§ 8.2 网络扫描

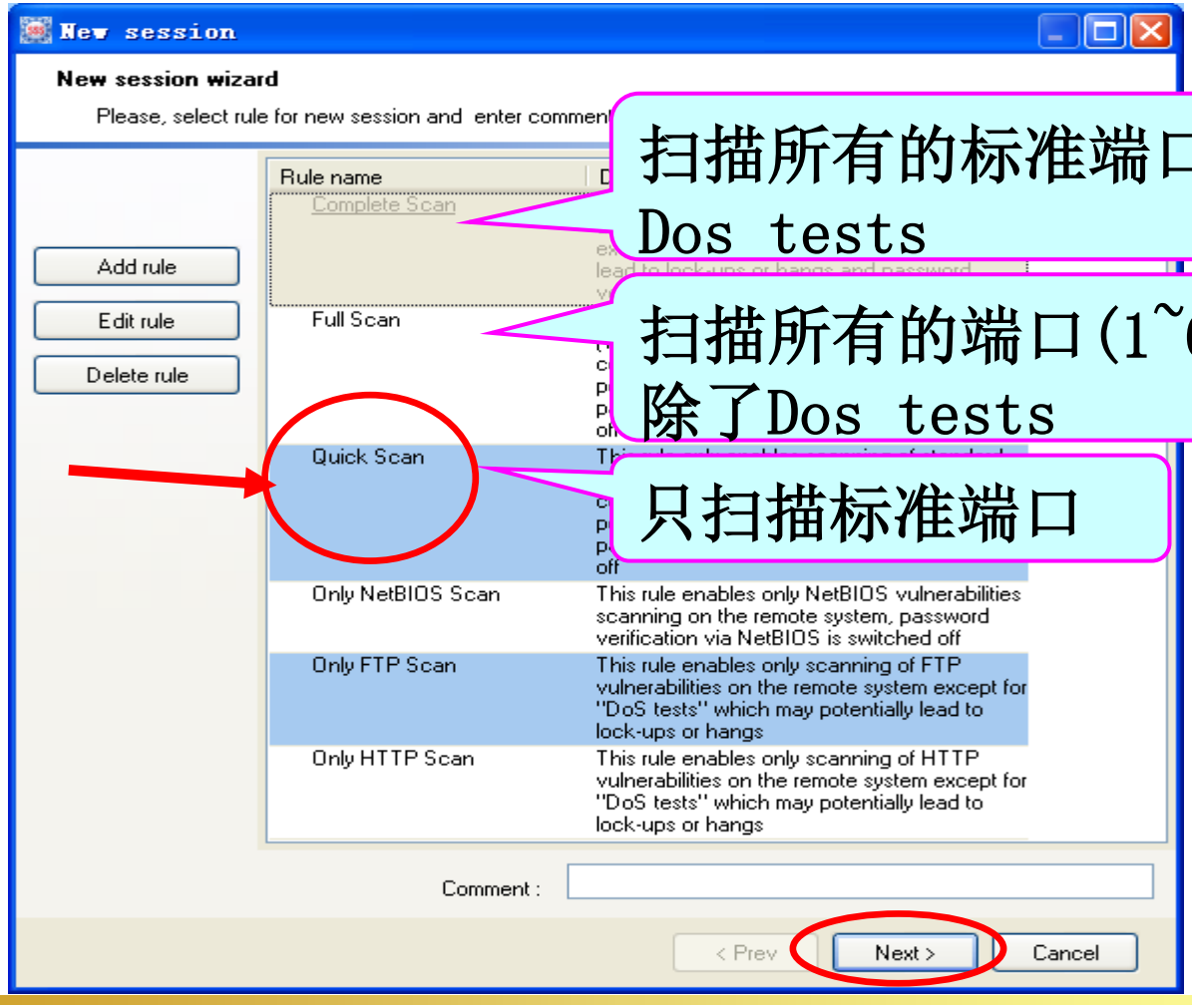
- 漏洞扫描——工具软件：SSS

主界面



§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



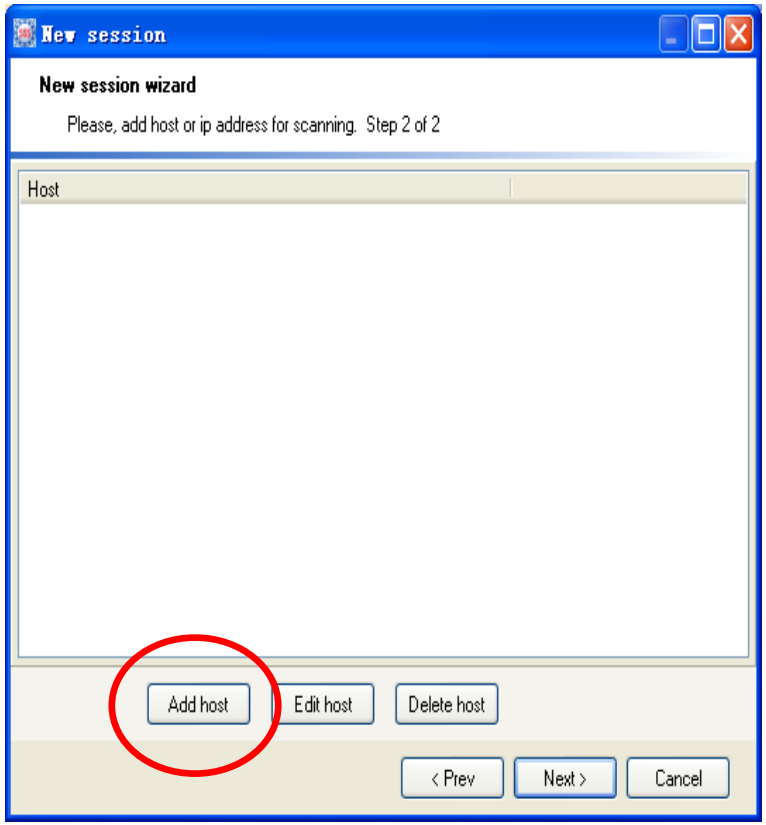
扫描所有的标准端口，除了Dos tests

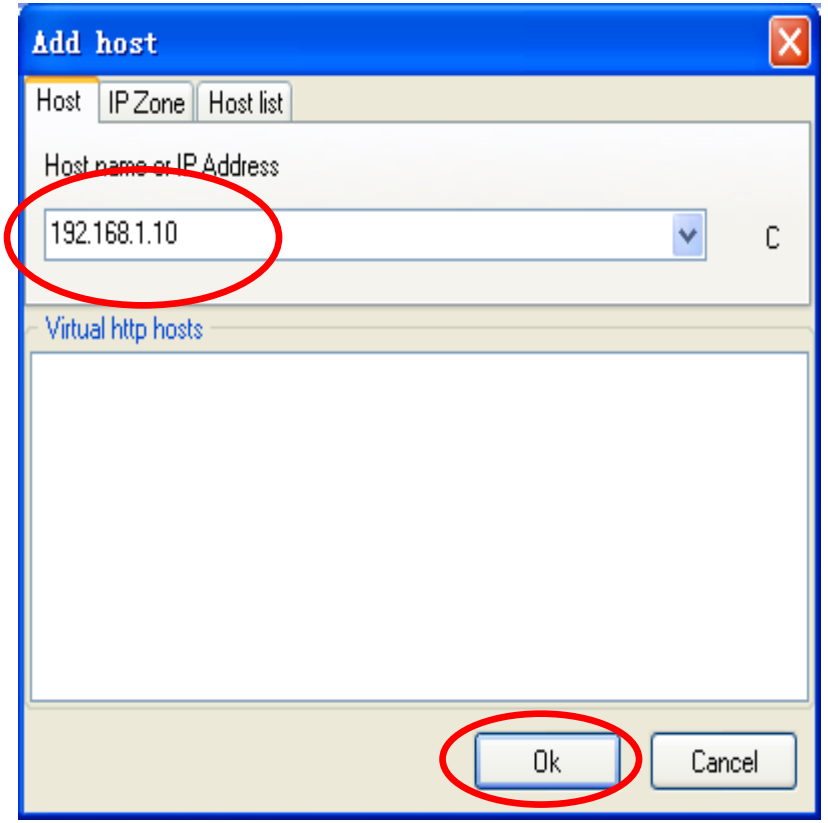
扫描所有的端口(1~65355)，除了Dos tests

只扫描标准端口

§ 8.2 网络扫描

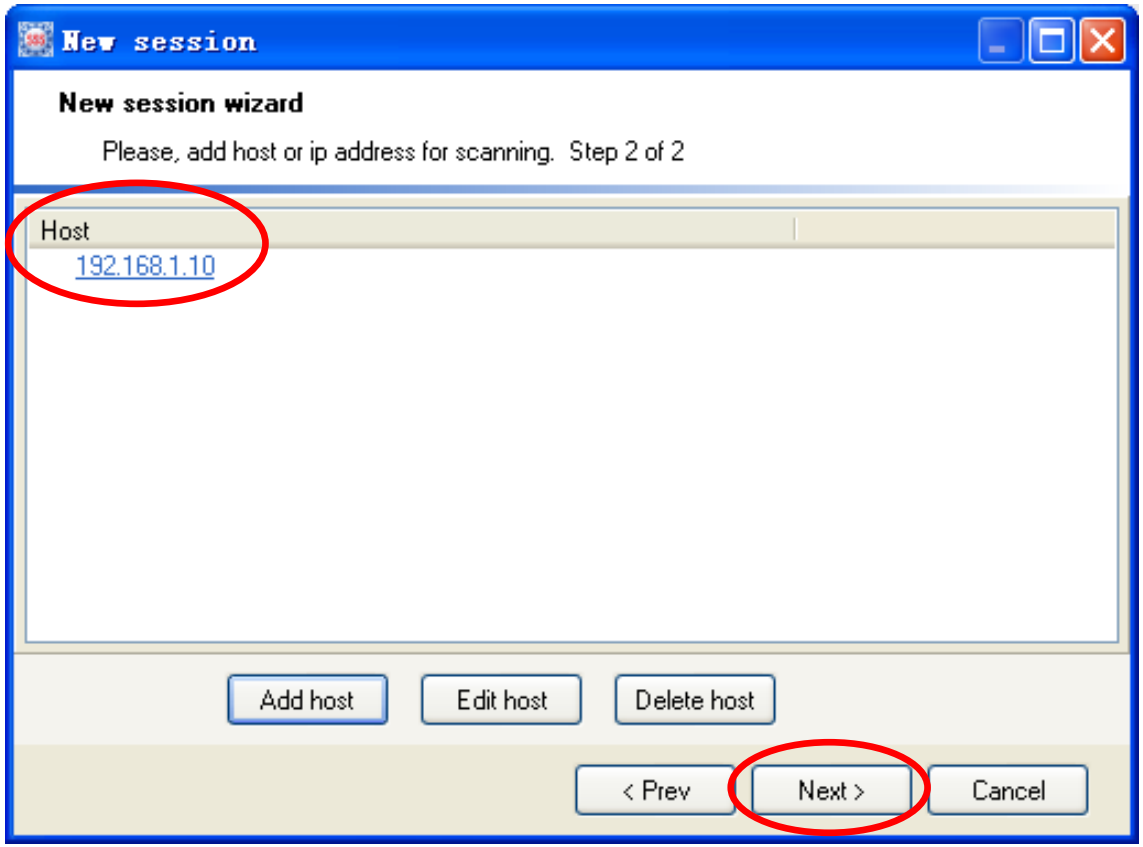
- 漏洞扫描——工具软件：SSS





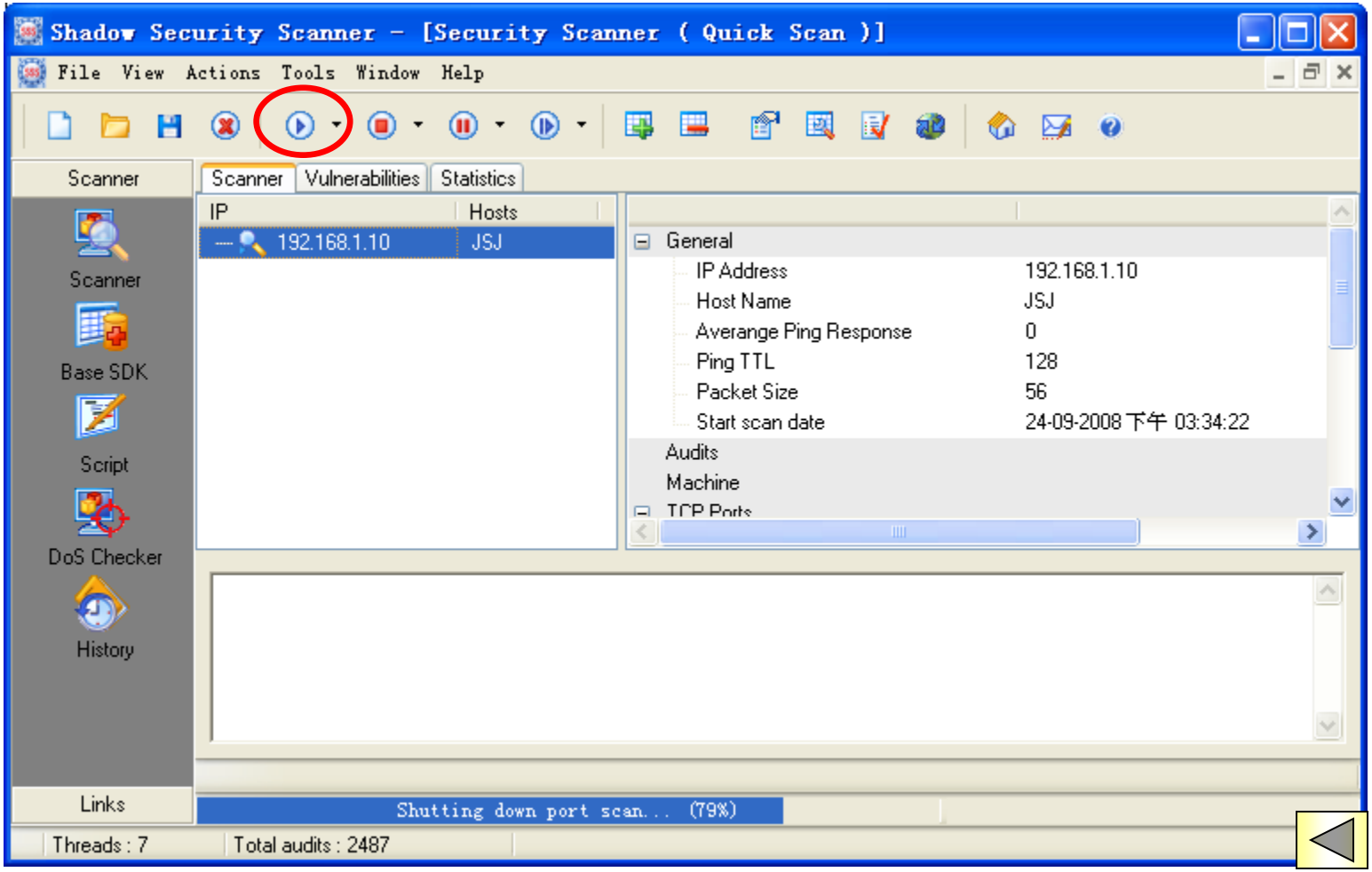
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



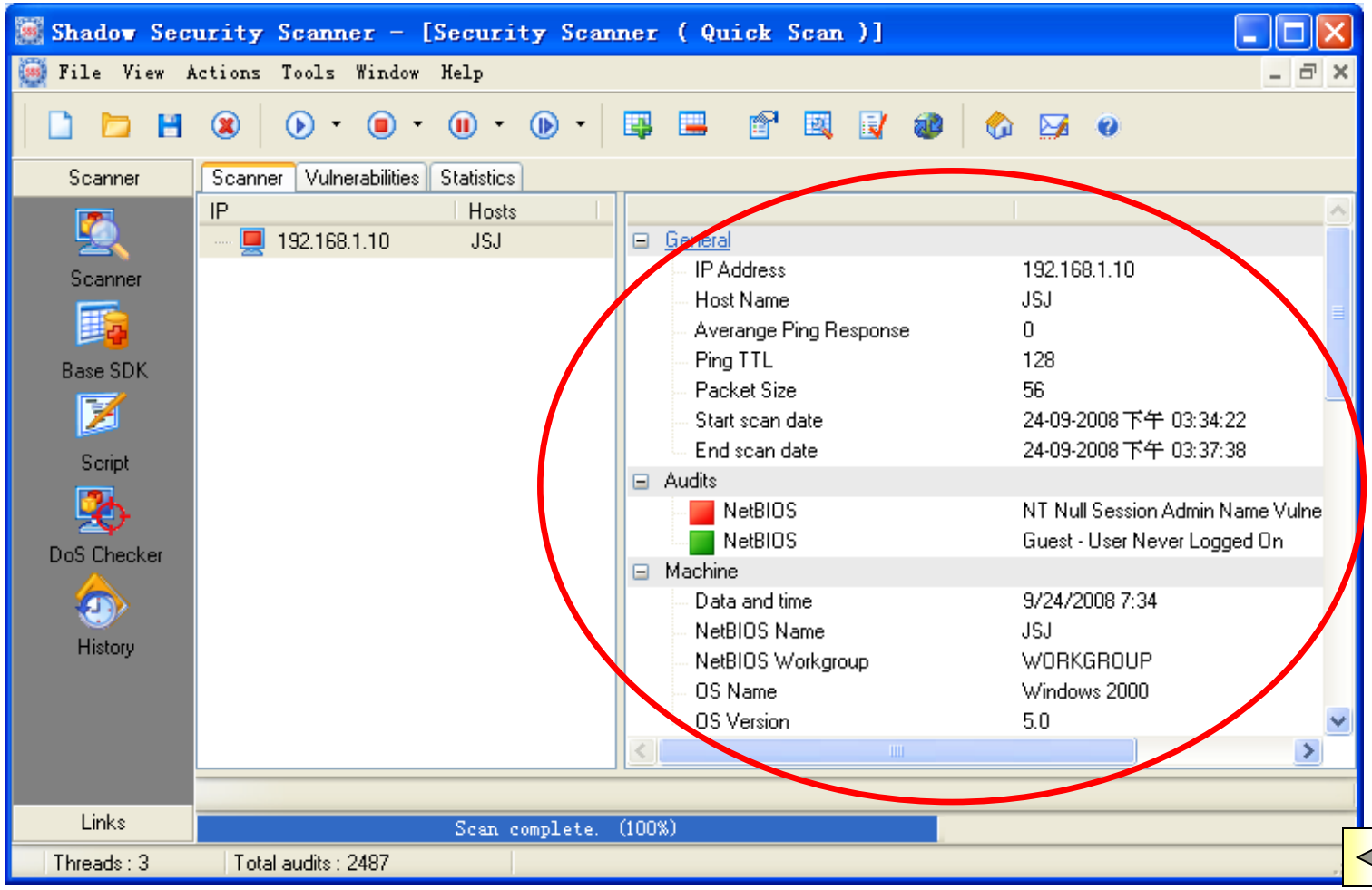
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



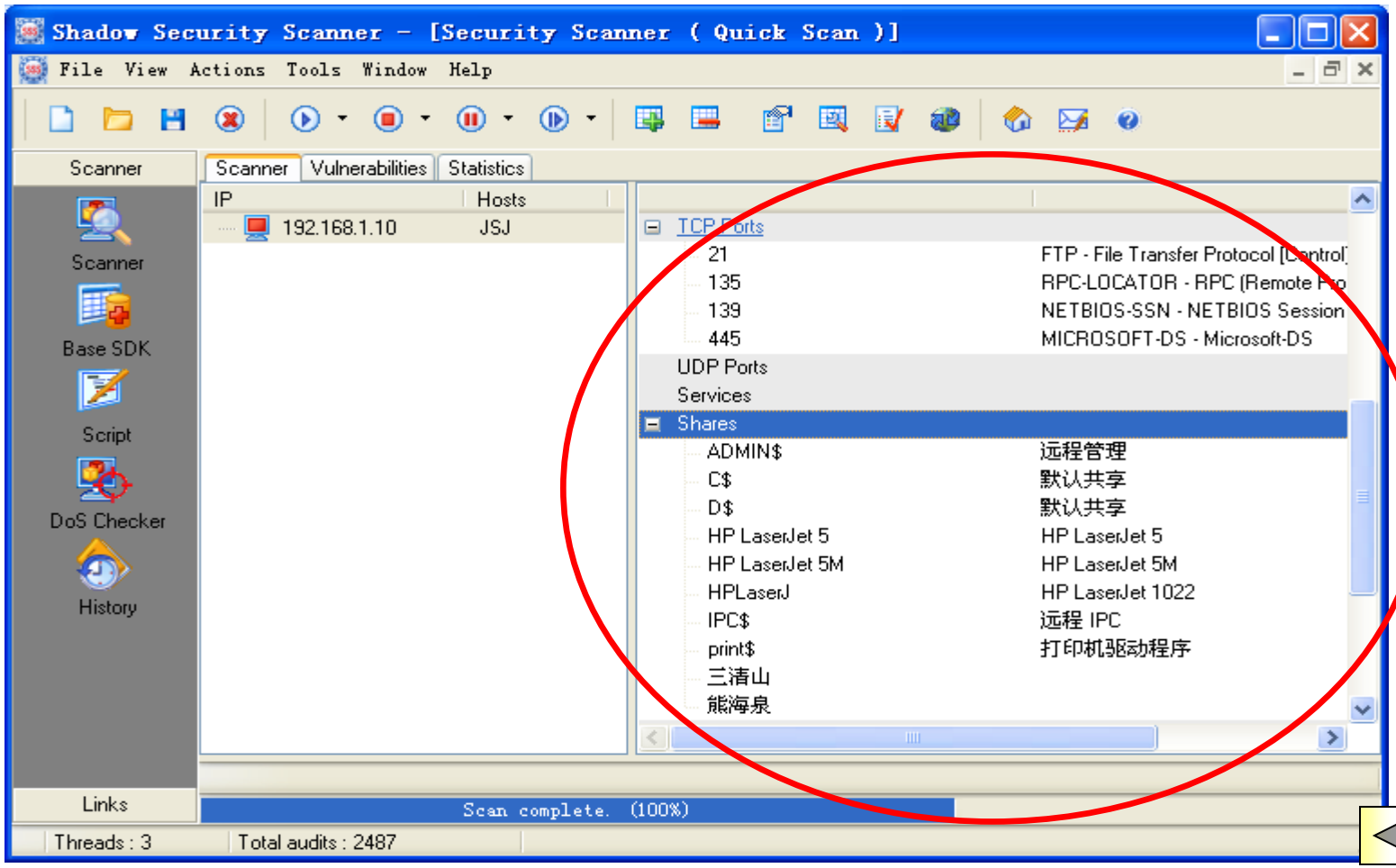
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



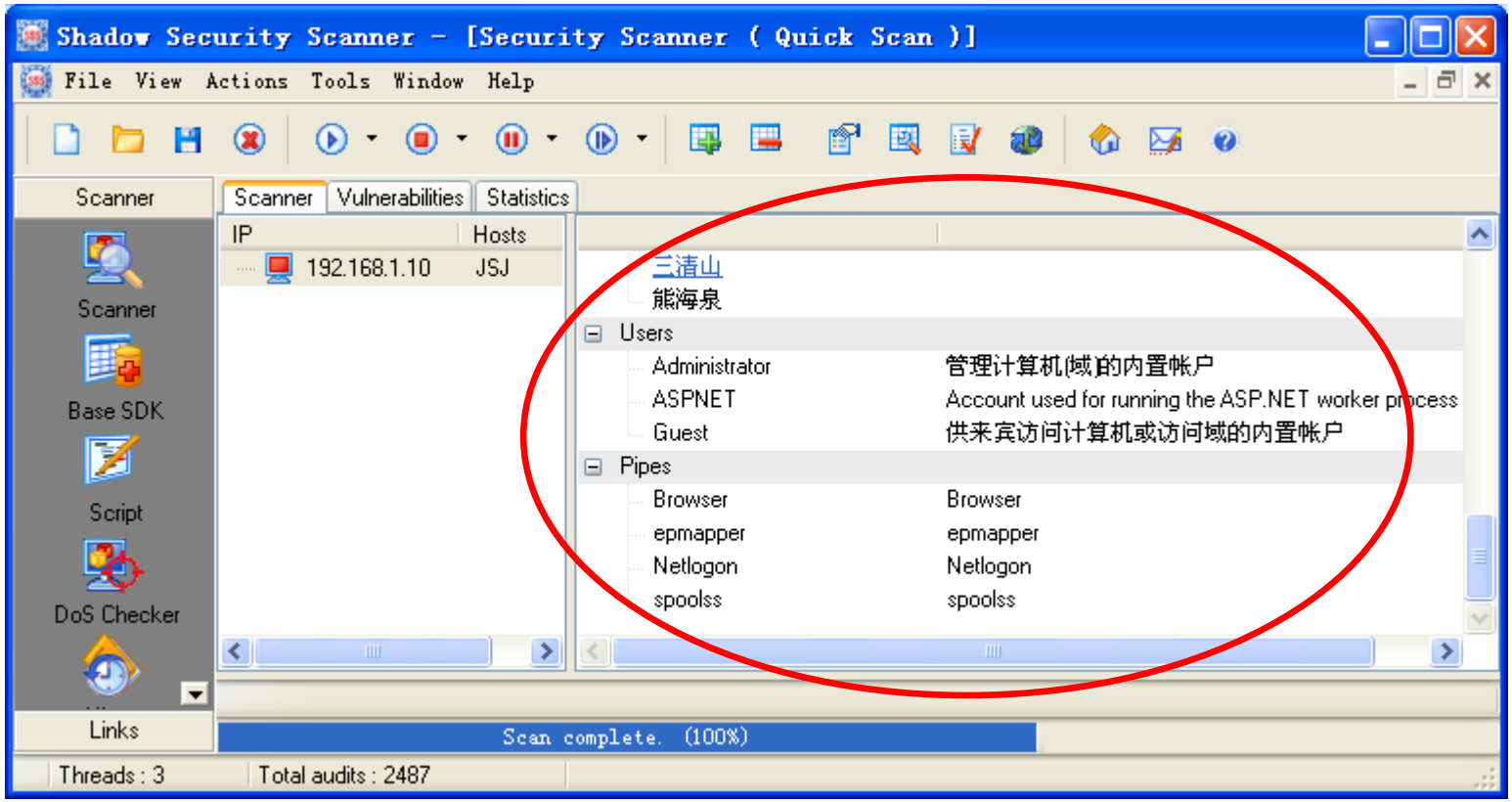
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



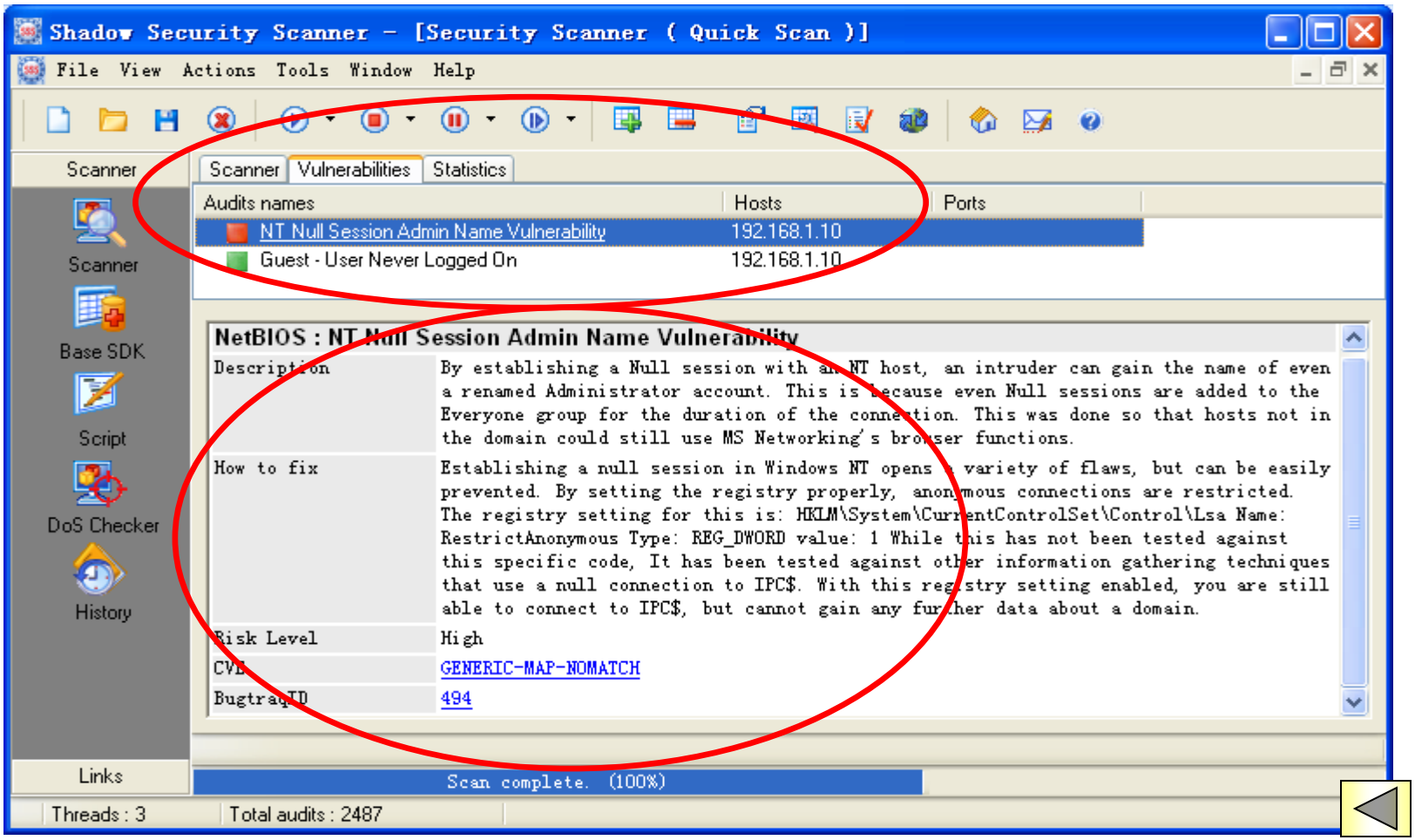
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



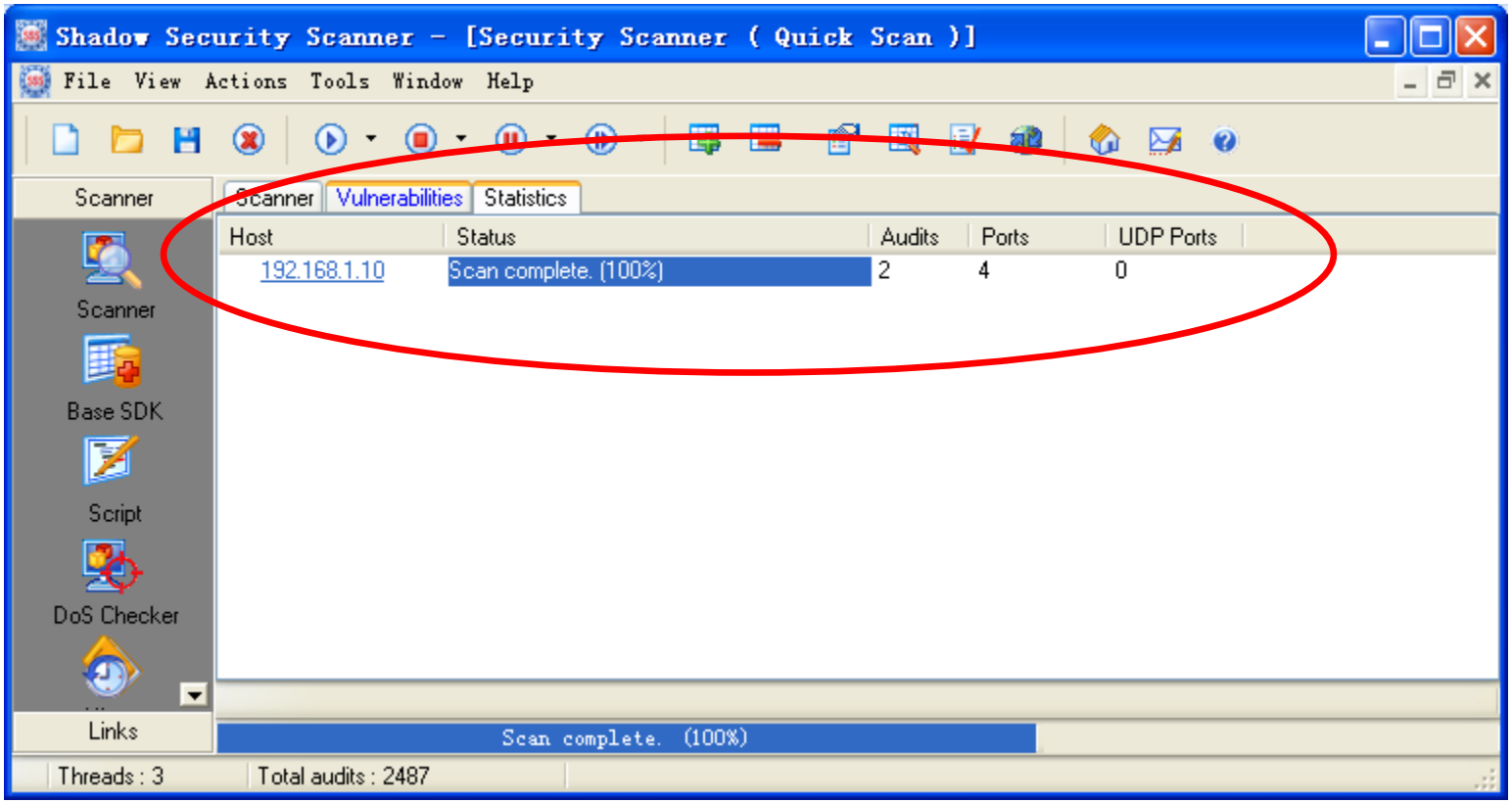
§ 8.2 网络扫描

- 漏洞扫描——工具软件：SSS



§ 8.2 网络扫描

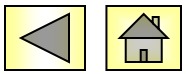
- 漏洞扫描——工具软件：SSS



§8.2 网络扫描

漏洞攻击的防范措施

- 安装防火墙，禁止访问不该访问的服务端口，使用NAT隐藏内部网络结构
- 安装入侵检测系统，检测漏洞攻击行为
- 安装安全评估系统，先于入侵者进行模拟漏洞攻击，以便及早发现漏洞并解决
- 提高安全意识，经常给操作系统和应用软件打补丁



§8.3 网络监听

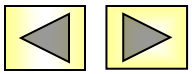
- 所谓网络监听就是获取在网络上传输的信息。通常，这种信息并不是特定发给自己计算机的。一般情况下，系统管理员为了有效地管理网络、诊断网络问题而进行网络监听。然而，黑客为了达到其不可告人的目的，也进行网络监听。
- 以太网中信息传输的原理：发送信息时，发送方将对所有的主机进行广播，广播包的包头含有目的主机的物理地址，如果地址与主机不符，则该主机对数据包不予理睬，只有当地址与主机自己的地址相同时主机才会接受该数据包，但网络监听程序可以使得主机对所有通过它的数据进行接收或改变。
- 网络监听使得进行监听的机器响应速度变得非常慢。

§8.3 网络监听

- 网络监听的作用
  - 可以截获用户口令
  - 可以截获秘密的或专用的信息
  - 可以用来攻击相邻的网络
  - 可以对数据包进行详细的分析
  - 可以分析出目标主机采用了哪些协议

§8.3 网络监听

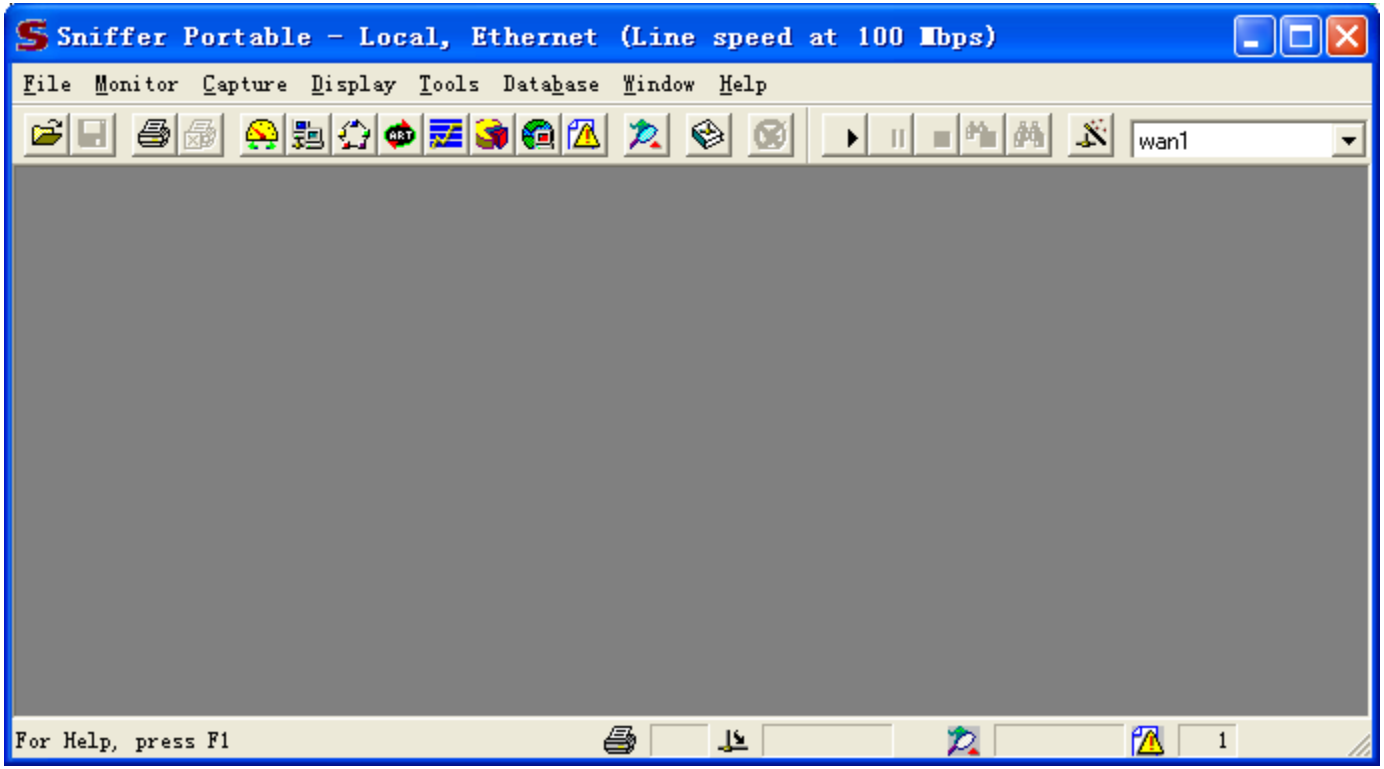
- 常用的监听工具
  - Sniffer Pro
  - Iris
  - Win Sniffer
  - pswmonitor
  - fssniffer



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

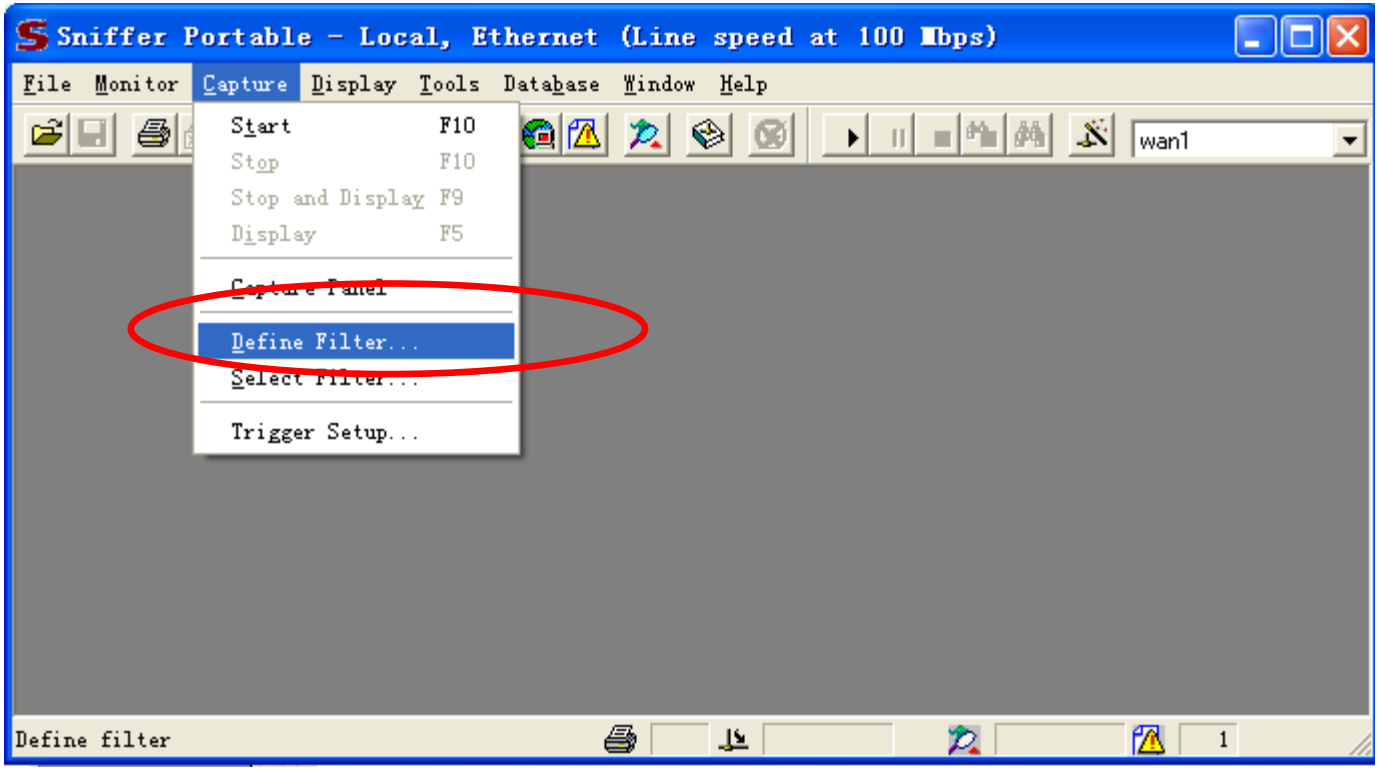
主界面



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

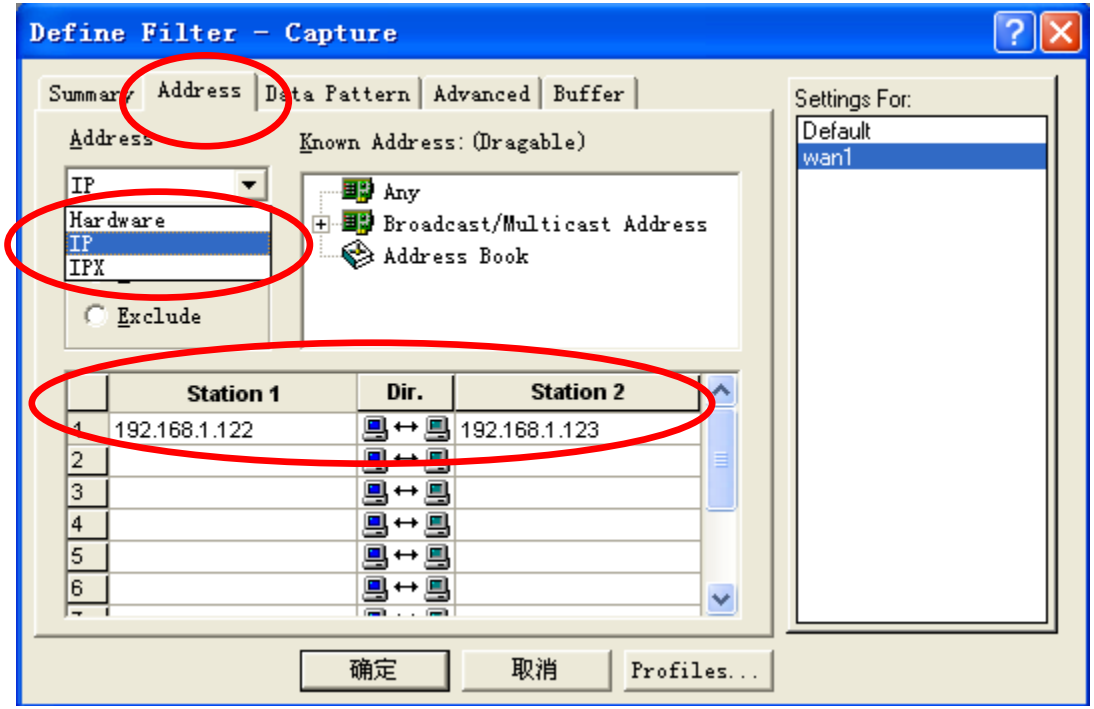
  捕获→定义过滤器



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

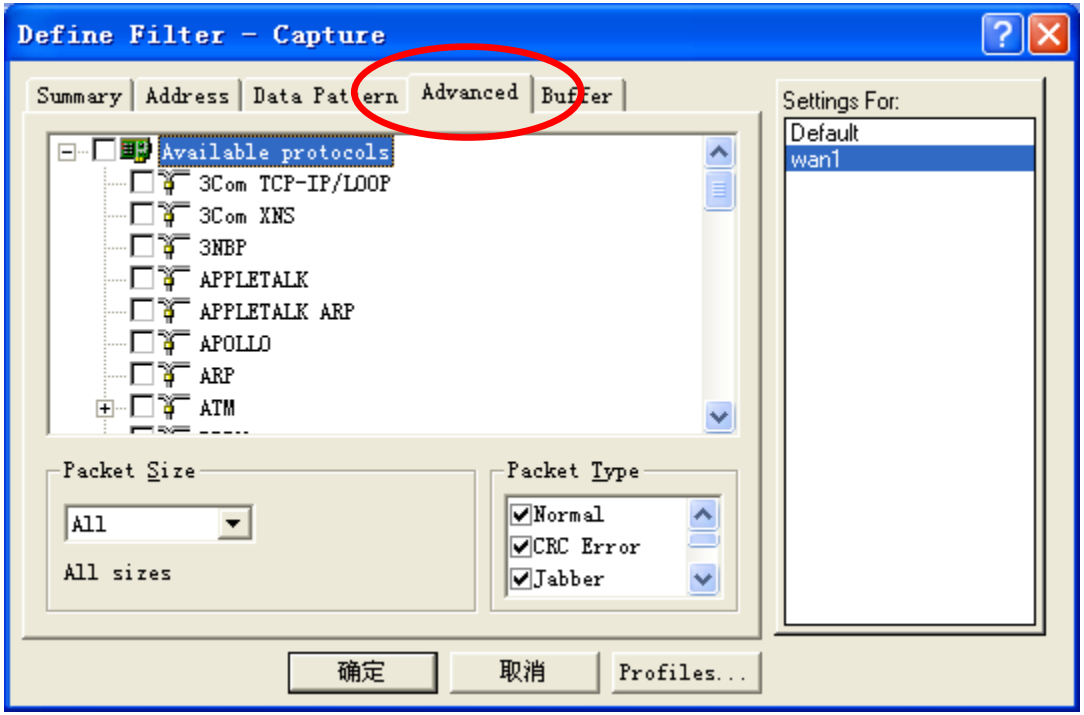
  设置捕获条件→IP地址条件



§8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

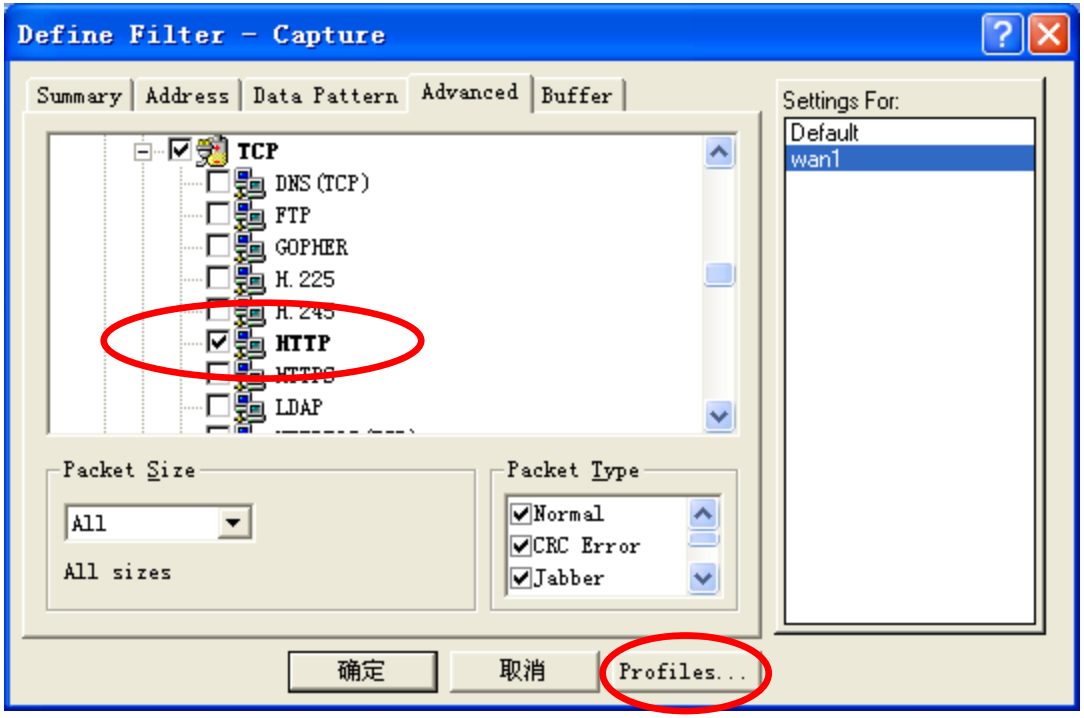
设置捕获条件→协议捕获编辑



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

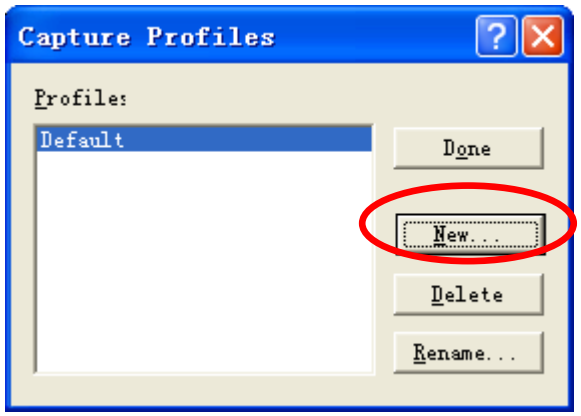
  如捕获http数据包

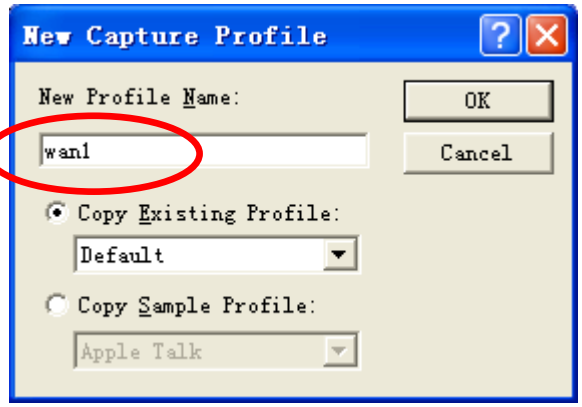


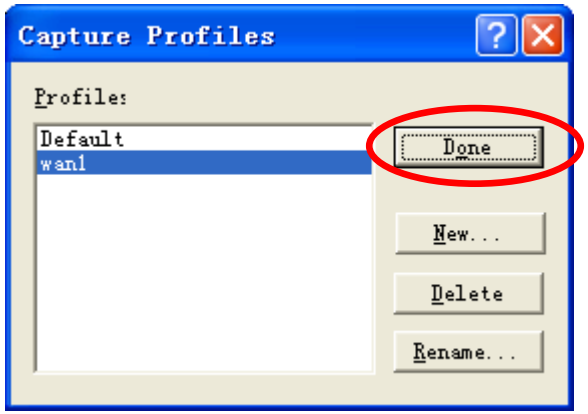
§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

保存过滤规则条件



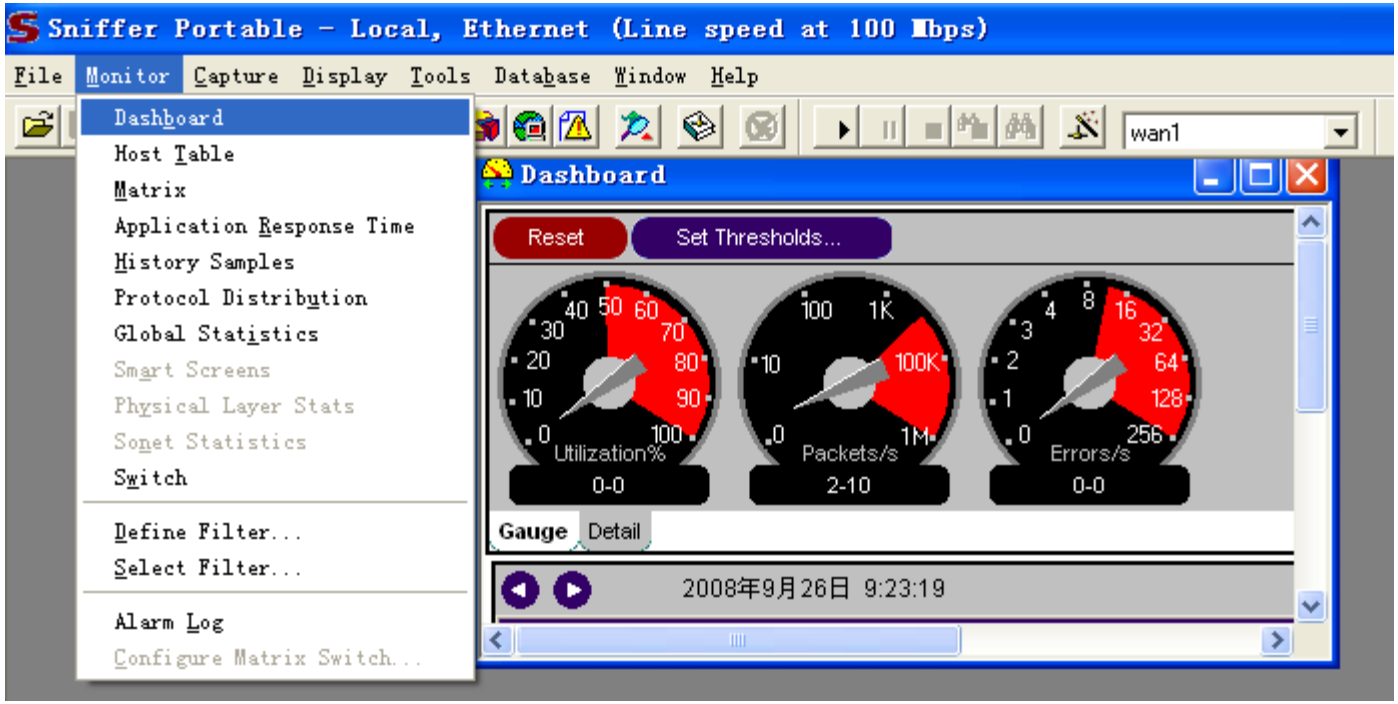




§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

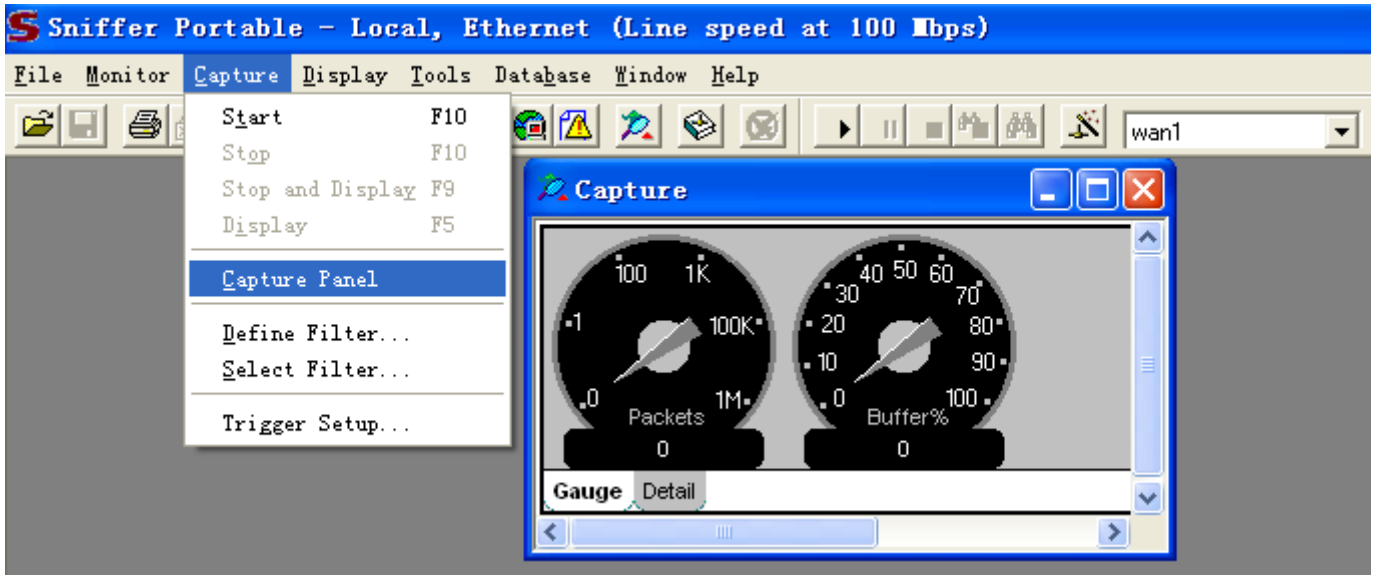
  监视器→仪表板，显示捕包的个数



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

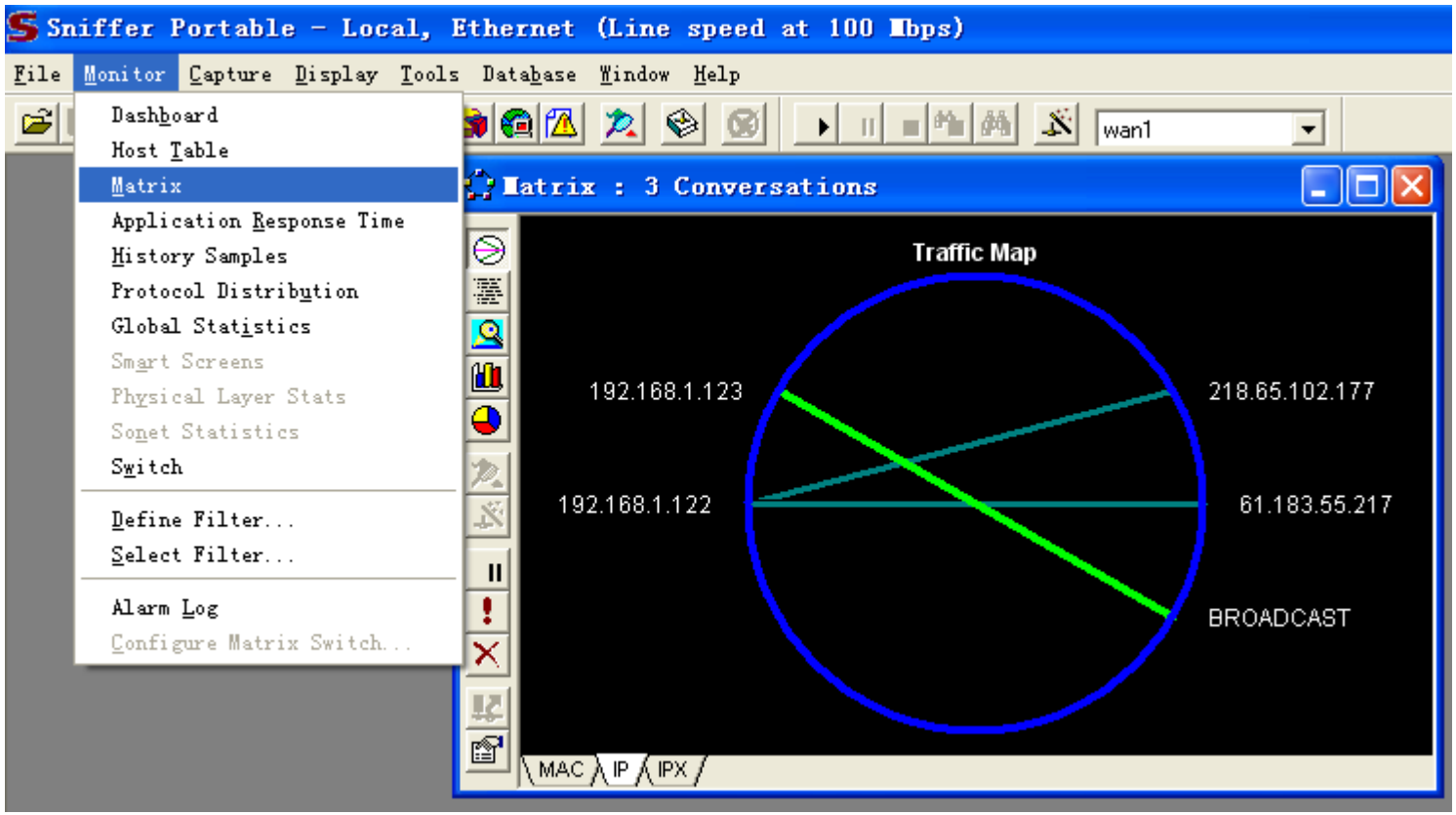
  捕获→面板，查看捕获报文的数量和缓冲区的利用率



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

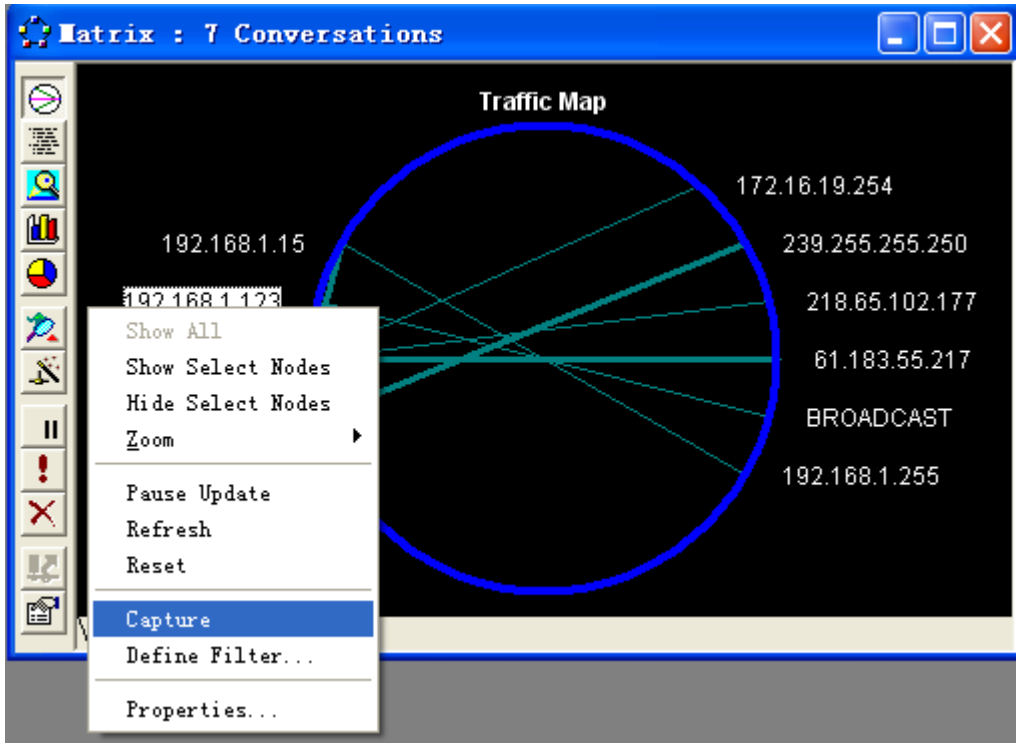
  监视器→矩阵，出现主机所在局域网的所有通信连接



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

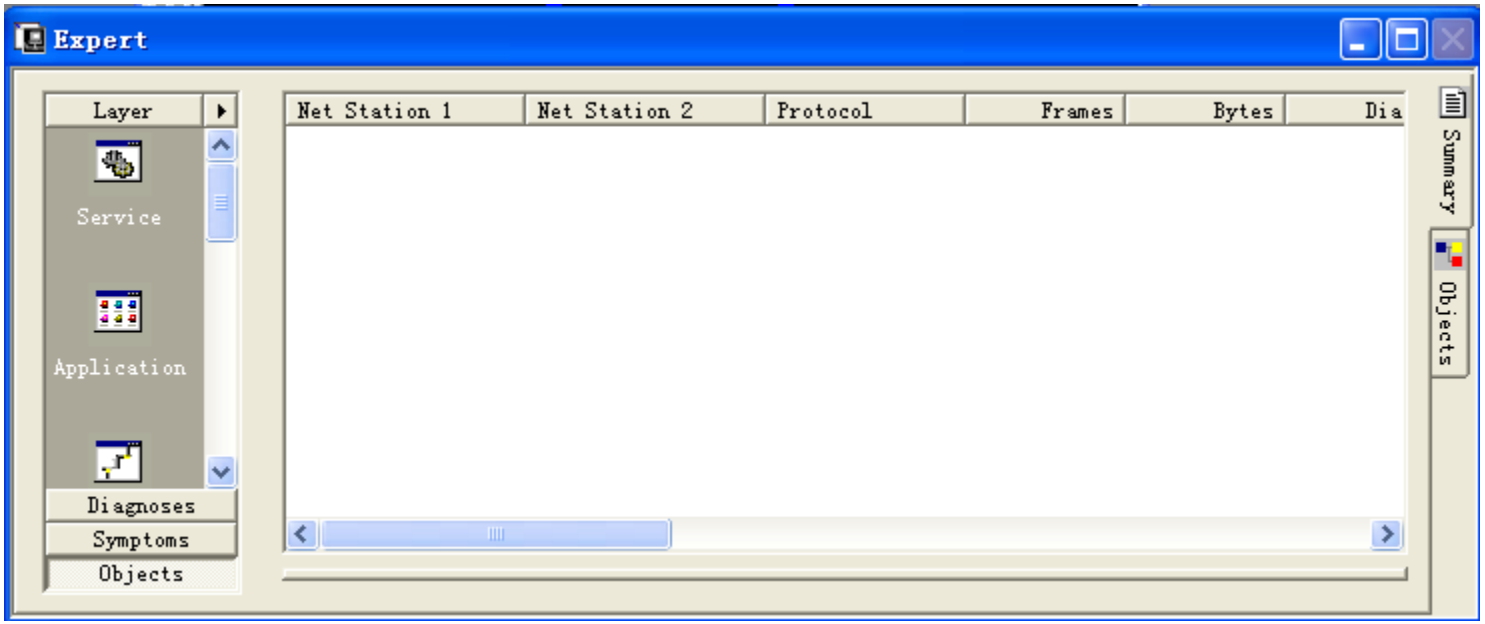
选中要监视的IP地址，右击选择“捕获”



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro

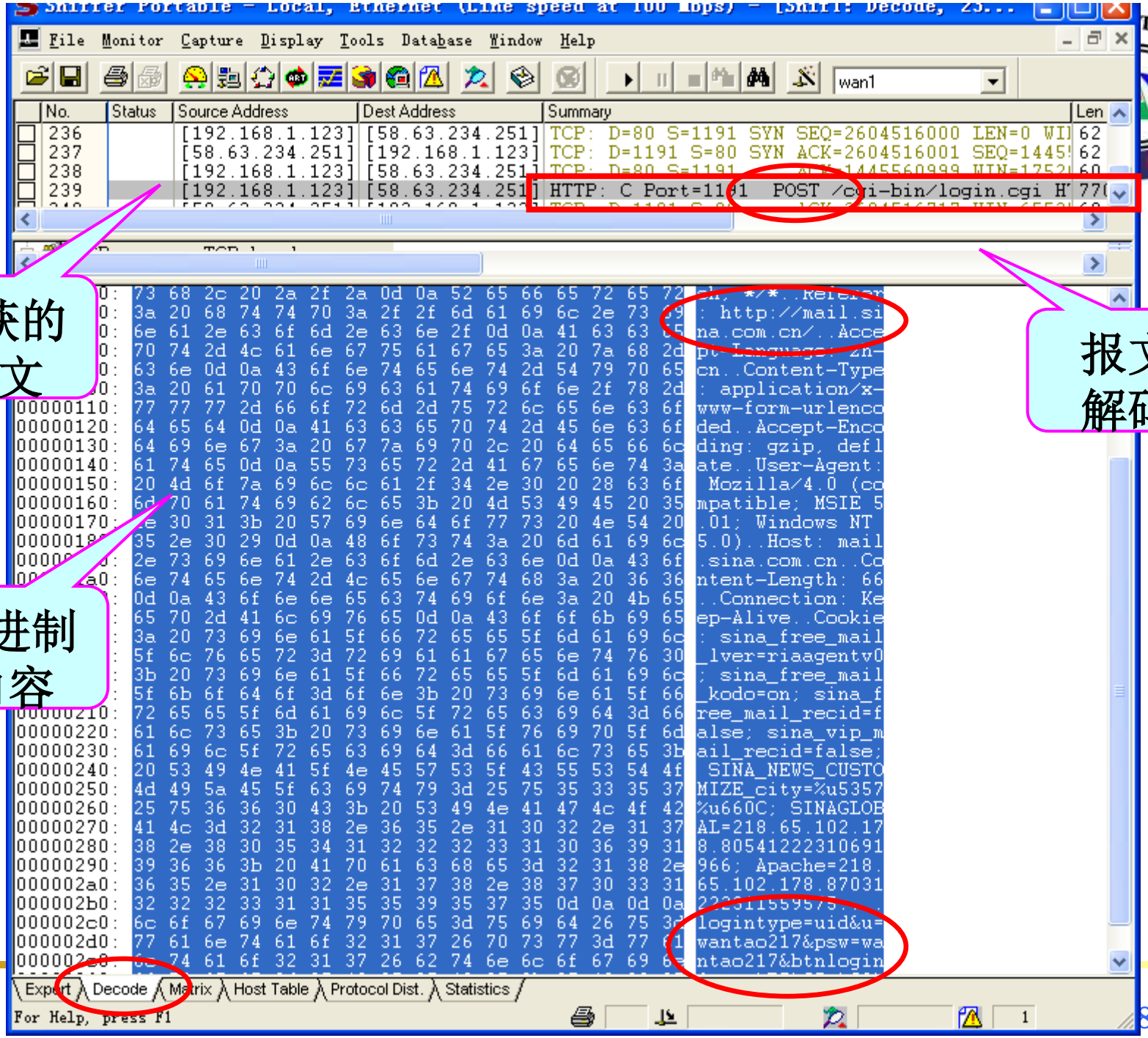
  专家分析系统进行数据包分析



§ 8.3 网络监听

- 网络嗅探——工具软件Sniffer Pro




捕获的报文
二进制内容
报文解码
File Monitor Capture Display Tools Database Window Help
wan1
No. Status Source Address Dest Address Summary Len
236 [192.168.1.123] [58.63.234.251] TCP: D=80 S=1191 SYN SEQ=2604516000 LEN=0 WI 62
237 [58.63.234.251] [192.168.1.123] TCP: D=1191 S=80 SYN ACK=2604516001 SEQ=1445 62
238 [192.168.1.123] [58.63.234.251] TCP: D=80 S=1191 ACK=1445560999 WIN=1752 60
239 [192.168.1.123] [58.63.234.251] HTTP: C Port=1191 POST /cgi-bin/login.cgi H 77
Export Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1

§8.3 网络监听

- 针对网络嗅探攻击的防范措施
  - 安装VPN网关，防止对网间网信道进行嗅探
  - 对内部网络通信采取加密处理
  - 采用交换设备进行网络分段
  - 采取技术手段发现处于混杂模式的主机，发掘“鼹鼠”

§8.3 网络监听

网络监听的检测方法

- 对于怀疑运行监听程序的机器，用正确的IP地址和错误的物理地址去ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，处于监听状态的机器能接收。
- 往网上发大量不存在的物理地址的包，由于监听程序将处理这些包导致性能下降。通过比较前后该机器性能加以判断。这种方法难度比较大。
- 搜索所有主机上运行的进程。
- 搜索监听程序。若入侵者使用的是免费软件。管理员就可以检查目录，找出监听程序，但这很困难且费时。

§8.4 密码破解攻击

- 密码与用户账户的有效利用是网络安全性的最大问题之一。密码破解是描述在使用或不使用工具的情况下渗透网络、系统或资源以解锁用密码保护的资源的一个术语。
- 密码破解不一定涉及复杂的工具。它可能与找一张写有密码的贴纸一样简单，而这张纸就贴在显示器上或者藏在键盘底下。另一种暴力技术称为“垃圾搜寻”（Dumpster Diving），它基本上就是一个攻击者把垃圾搜寻一遍以找出可能含有密码的废弃文档。

§8.4 密码破解攻击

- 密码破解的常见技术
  - 字典攻击
  - 混合攻击
  - 暴力攻击

§8.4 密码破解攻击

- 密码破解的常见技术
  - 字典攻击

    到目前为止，一个简单的字典攻击（Dictionary Attack）是闯入机器的最快方法。字典文件（一个充满字典文字的文本文件）被装入破解应用程序（如LOphtCrack），它是根据由应用程序定位的用户账户运行的。因为大多数密码通常是简单的，所以运行字典攻击通常足以实现目的。
  - 混合攻击
  - 暴力攻击

§8.4 密码破解攻击

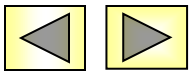
- 密码破解的常见技术
  - 字典攻击
  - 混合攻击

    混合攻击将数字和符号添加到文件名以成功破解密码。许多人只通过在当前密码后加一个数字来更改密码。其模式通常采用这一形式：第一月的密码是“cat”；第二个月的密码是“cat1”；第3个月的密码是“cat2”，依次类推。
  - 暴力攻击

§8.4 密码破解攻击

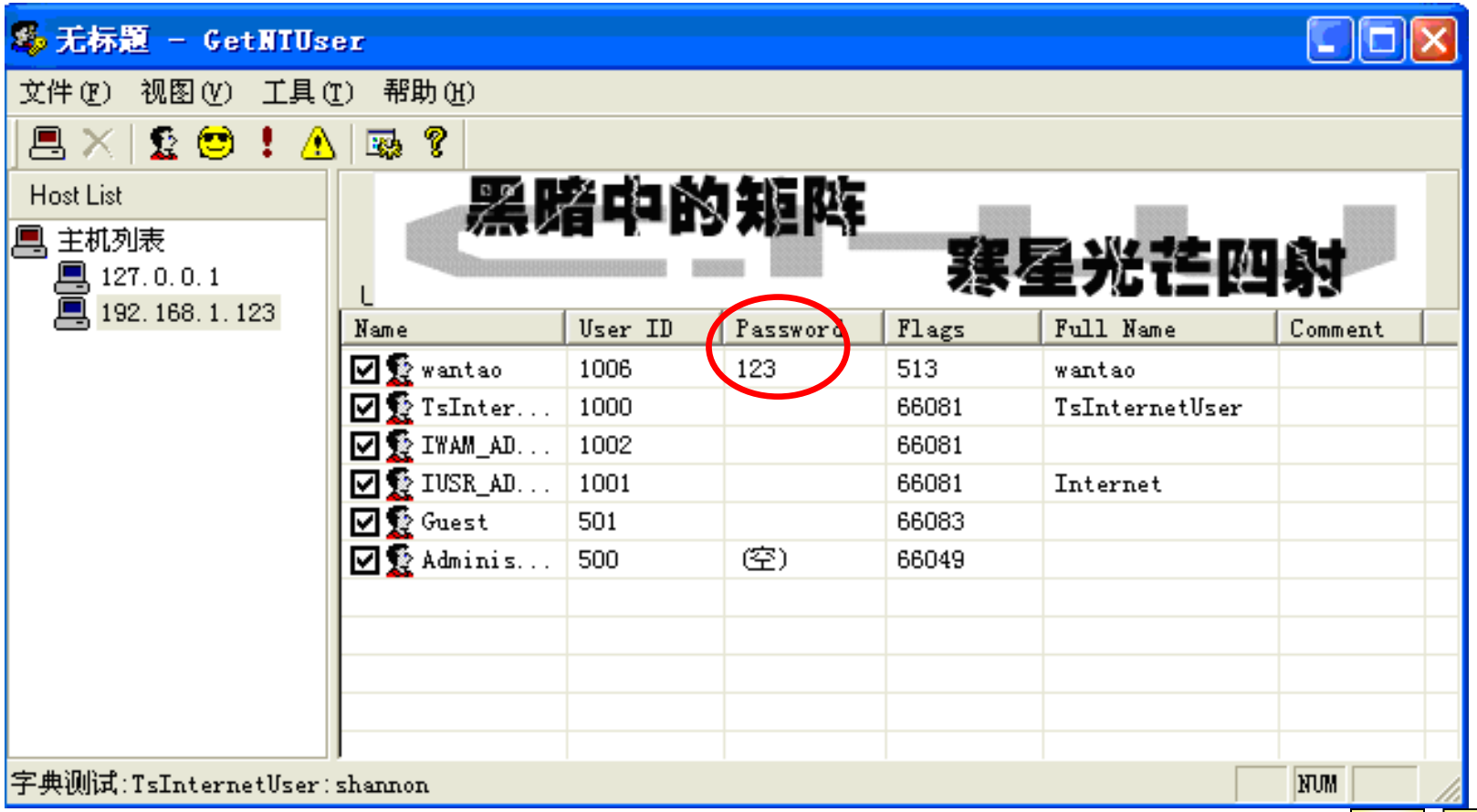
- 密码破解的常见技术
  - 字典攻击
  - 混合攻击
  - 暴力攻击

  暴力攻击（Brute Force Attack）是最全面的攻击形式，虽然它通常需要很长的时间工作，这取决于密码的复杂程度。根据密码的复杂程度，某些暴力攻击可能花费一个星期的时间。



§8.4 密码破解攻击

- 破解操作系统口令——工具软件GetNTUser



§8.4 密码破解攻击

- 破解操作系统口令——工具软件L0phtCrack

主界面



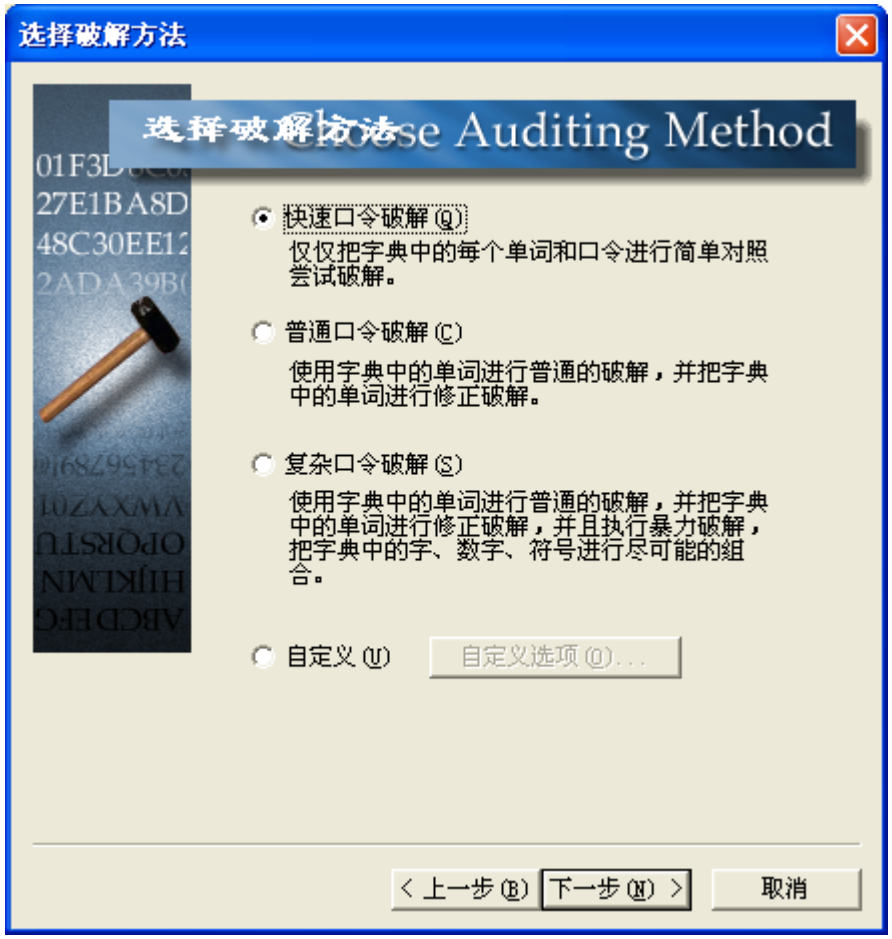
§8.4 密码破解攻击

- 破解操作系统口令——工具软件LOphtCrack



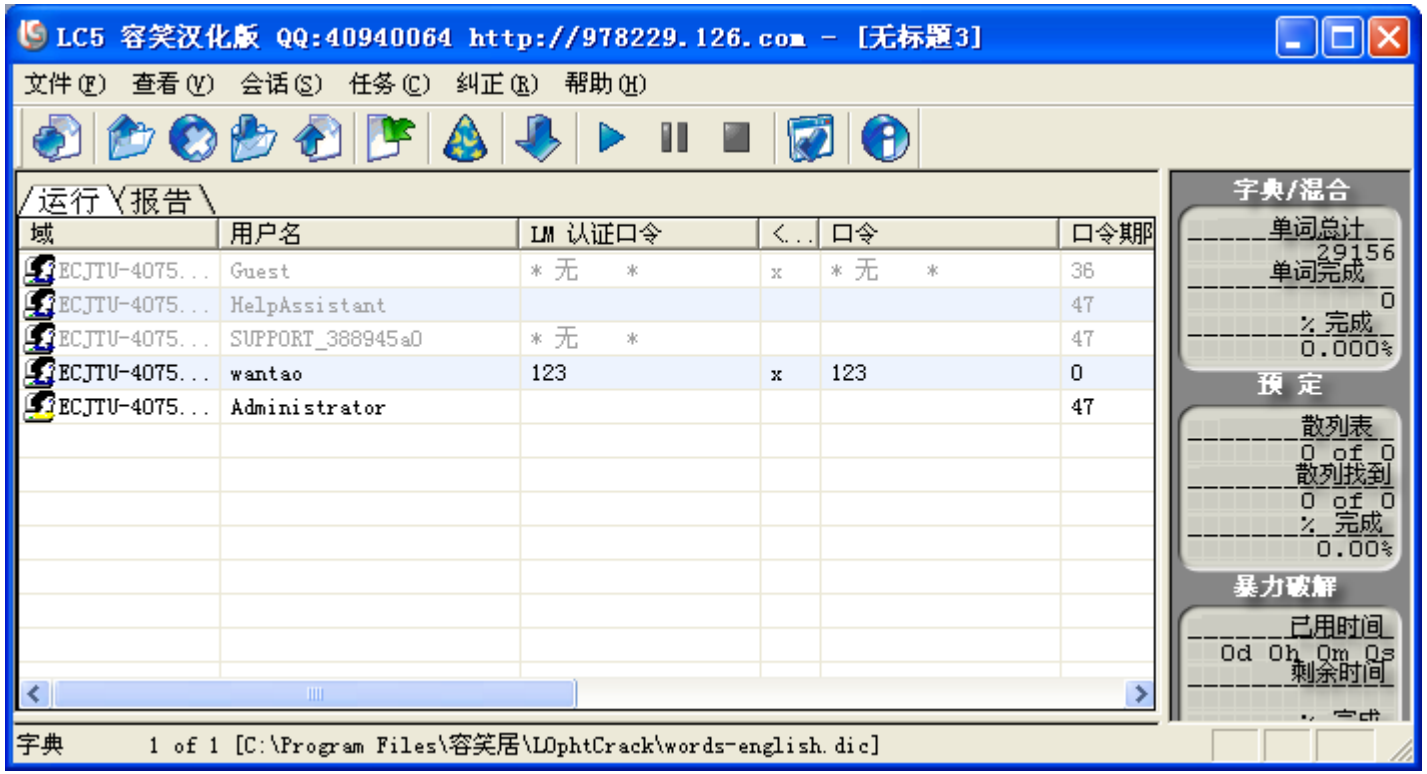
§8.4 密码破解攻击

- 破解操作系统口令——工具软件LOphtCrack



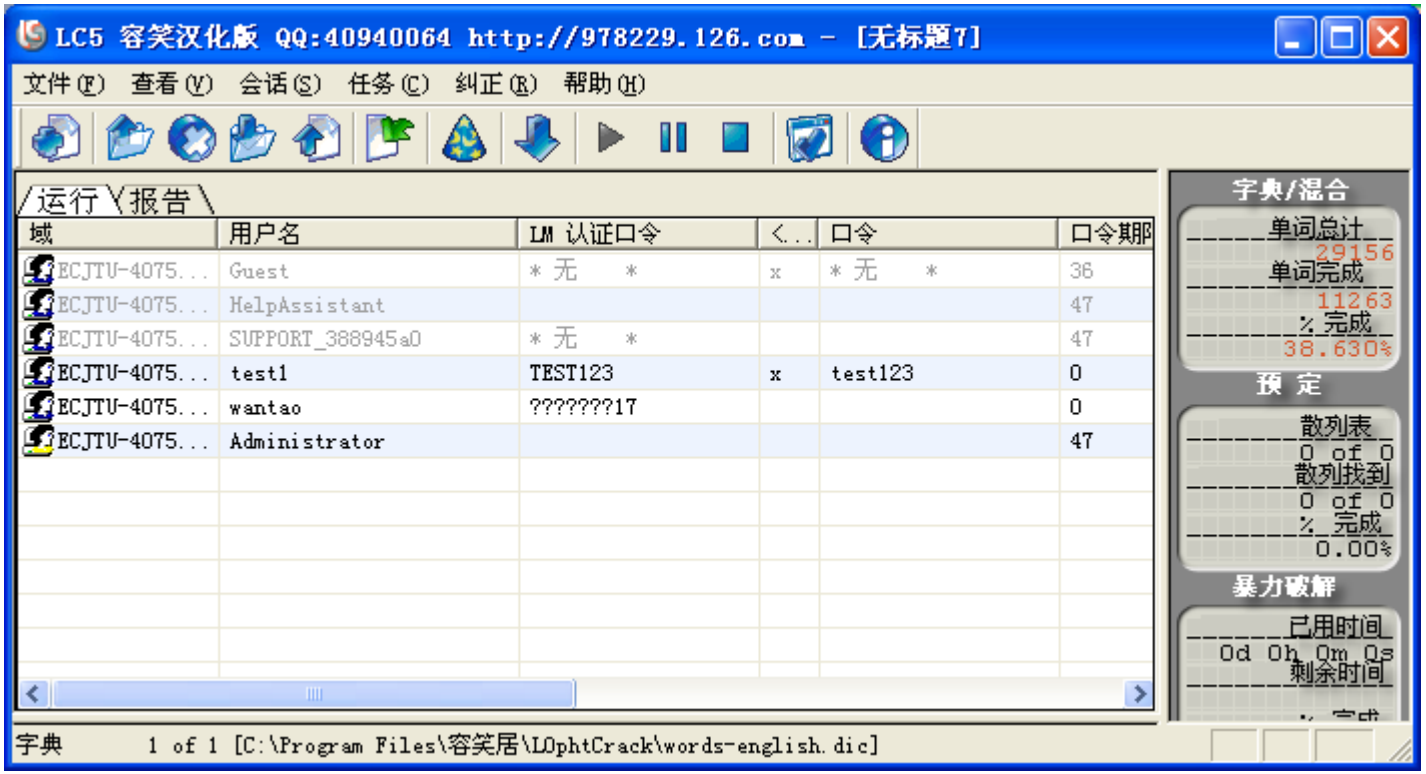
§8.4 密码破解攻击

- 破解操作系统口令——工具软件LOphtCrack



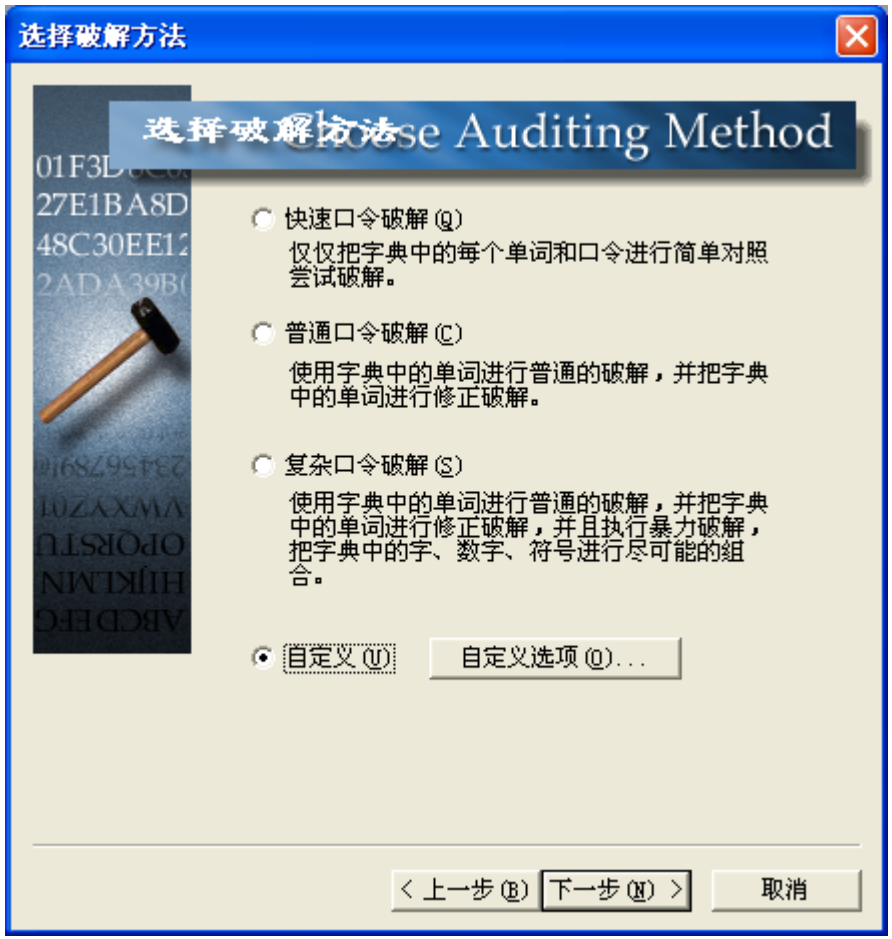
§8.4 密码破解攻击

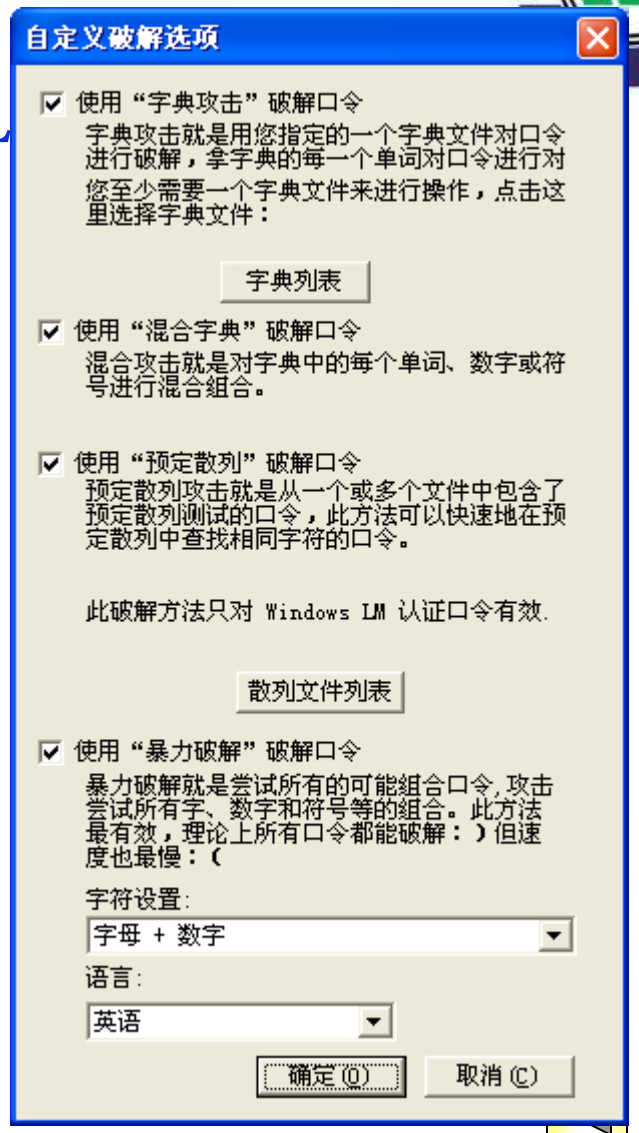
- 破解操作系统口令——工具软件LOphtCrack



§8.4 密码破解攻击

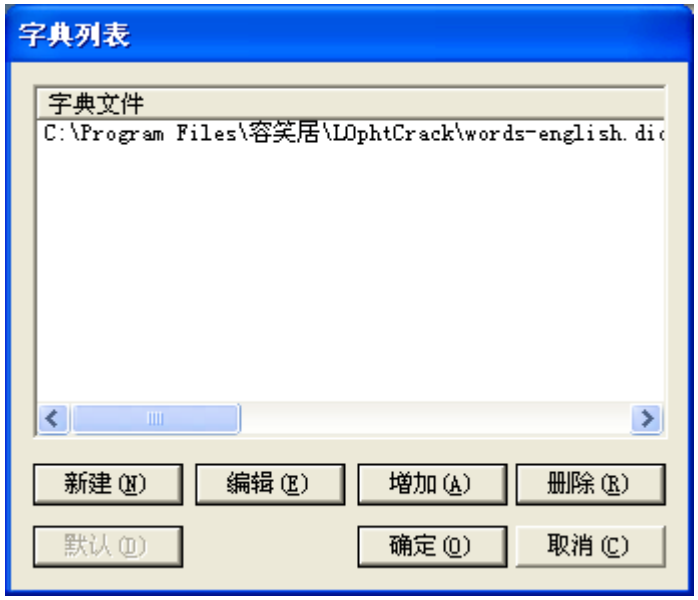
- 破解操作系统口令——工具软件L

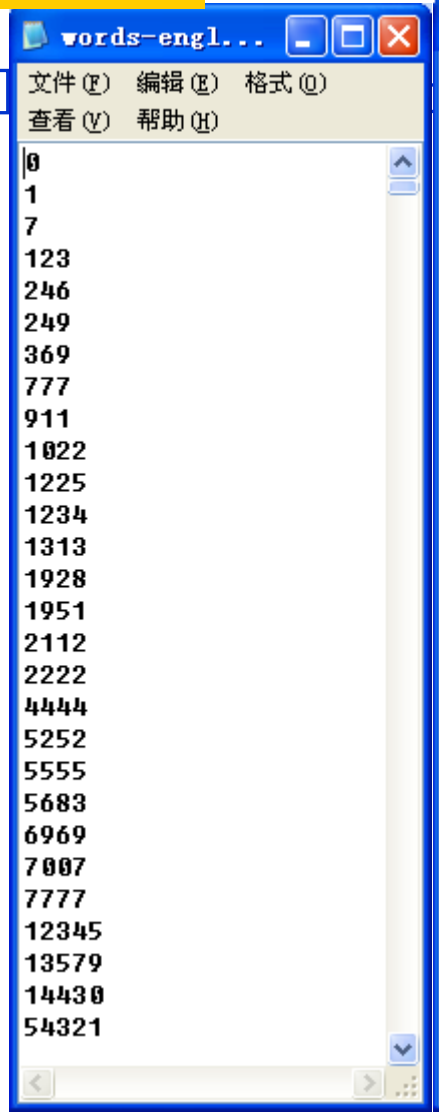


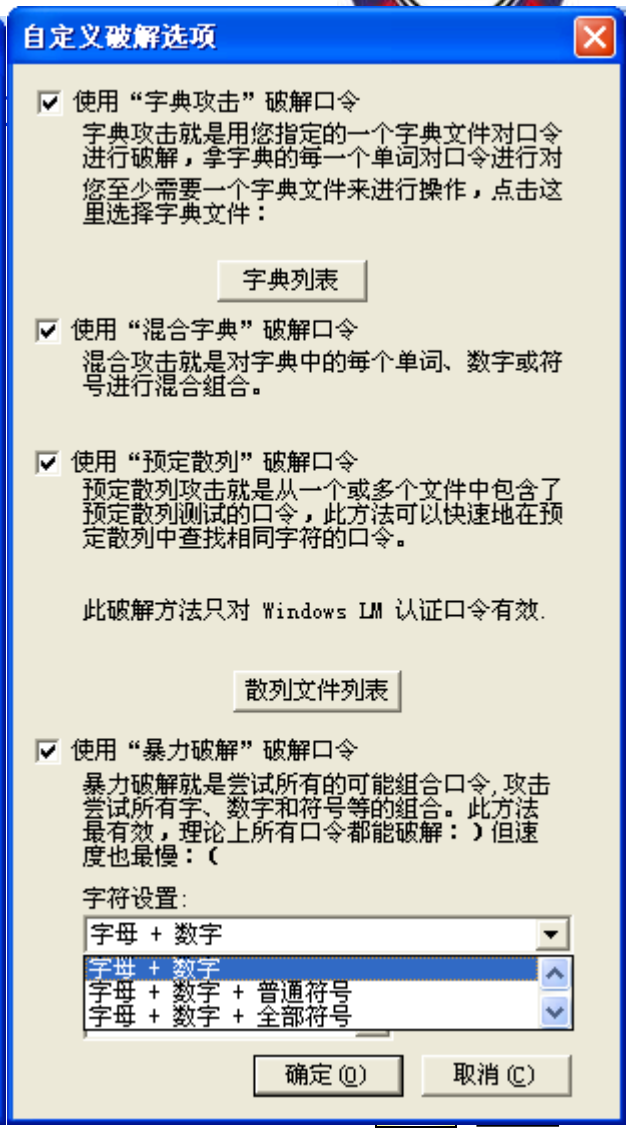


§8.4 密码破解攻击

- 破解操作系统口令——工



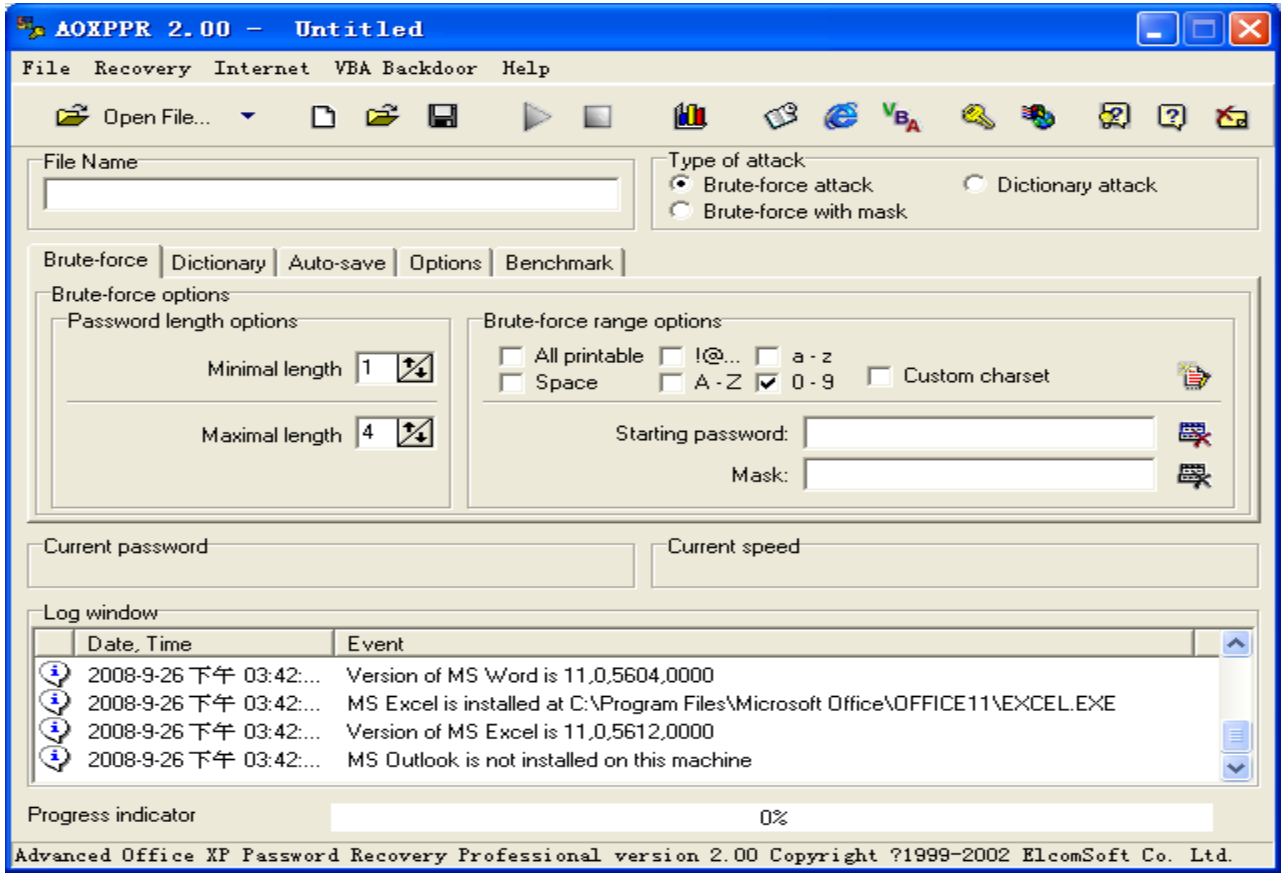




§8.4 密码破解攻击

- 破解Word文档密码——工具软件AOXPPR

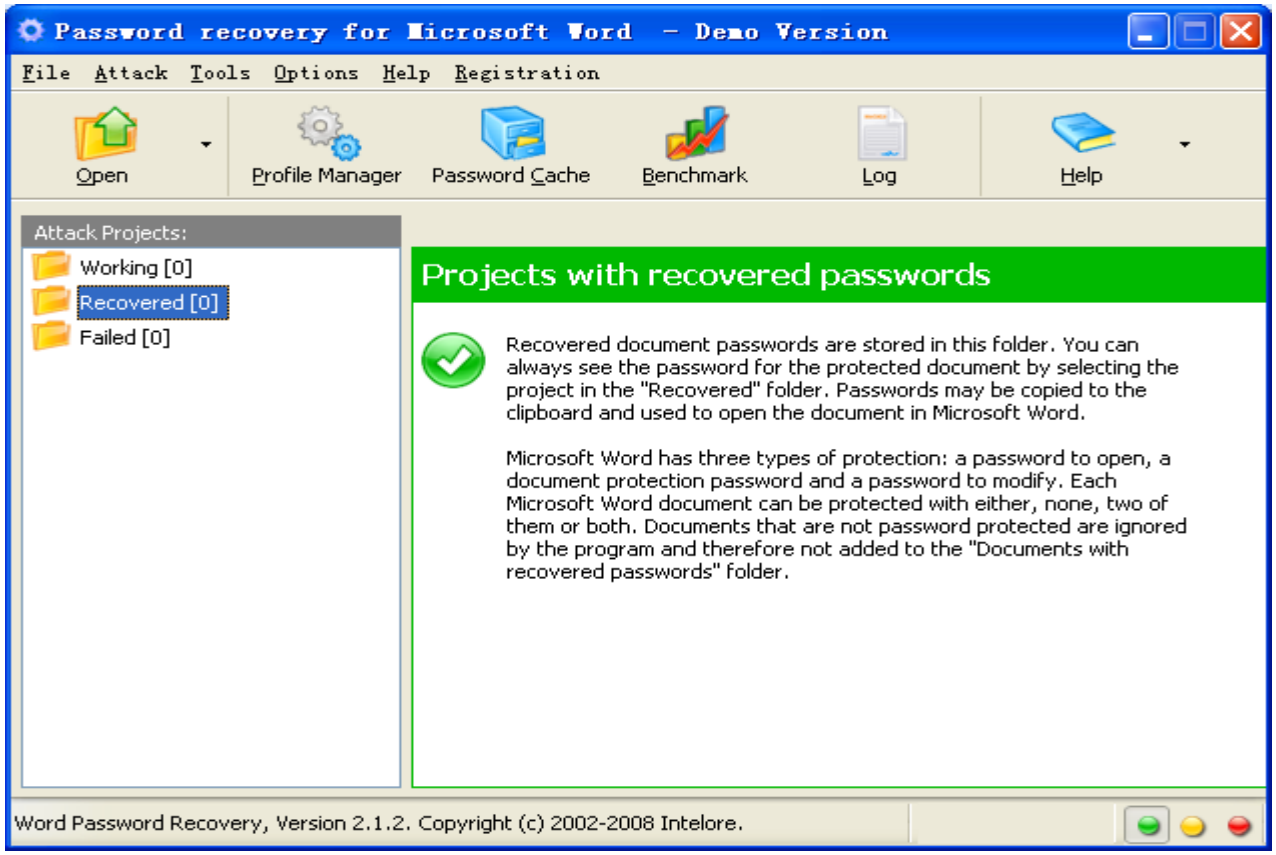
Advanced Office XP Password Recovery



§8.4 密码破解攻击

- 破解Word文档密码——工具软件

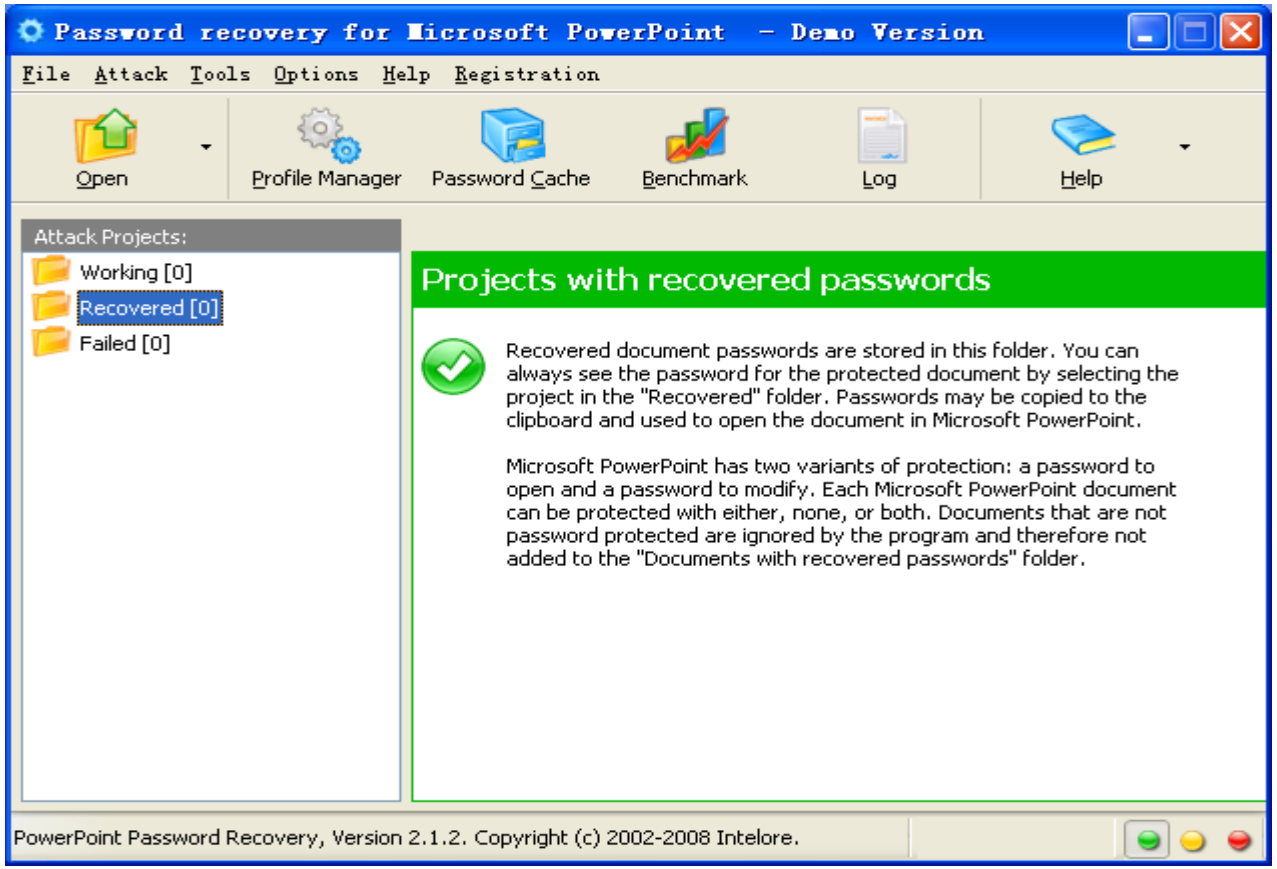
Password Recovery For Microsoft Word



§8.4 密码破解攻击

- 破解PPT文档密码——工具软件

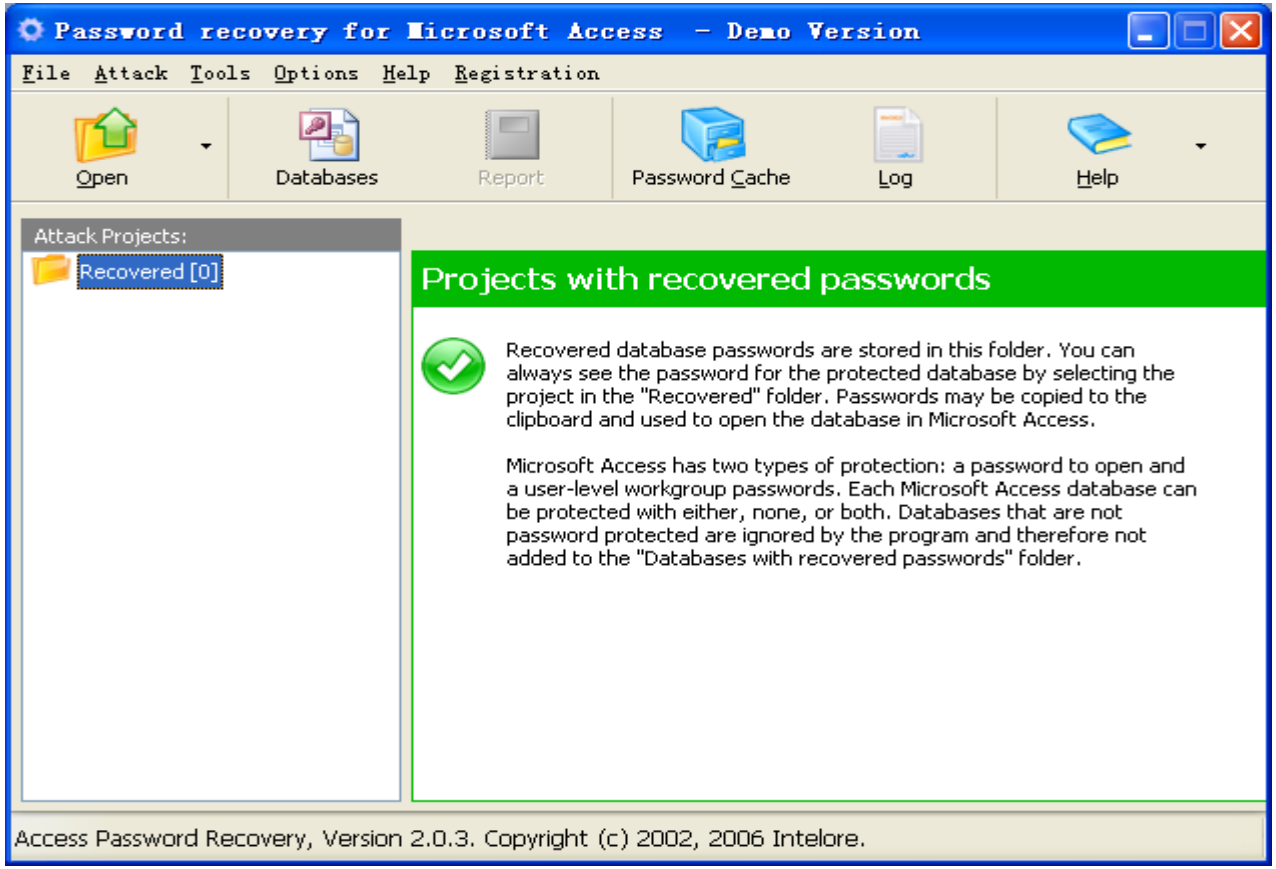
Password Recovery For Microsoft Powerpoint



§8.4 密码破解攻击

- 破解ACCESS文档密码——工具软件

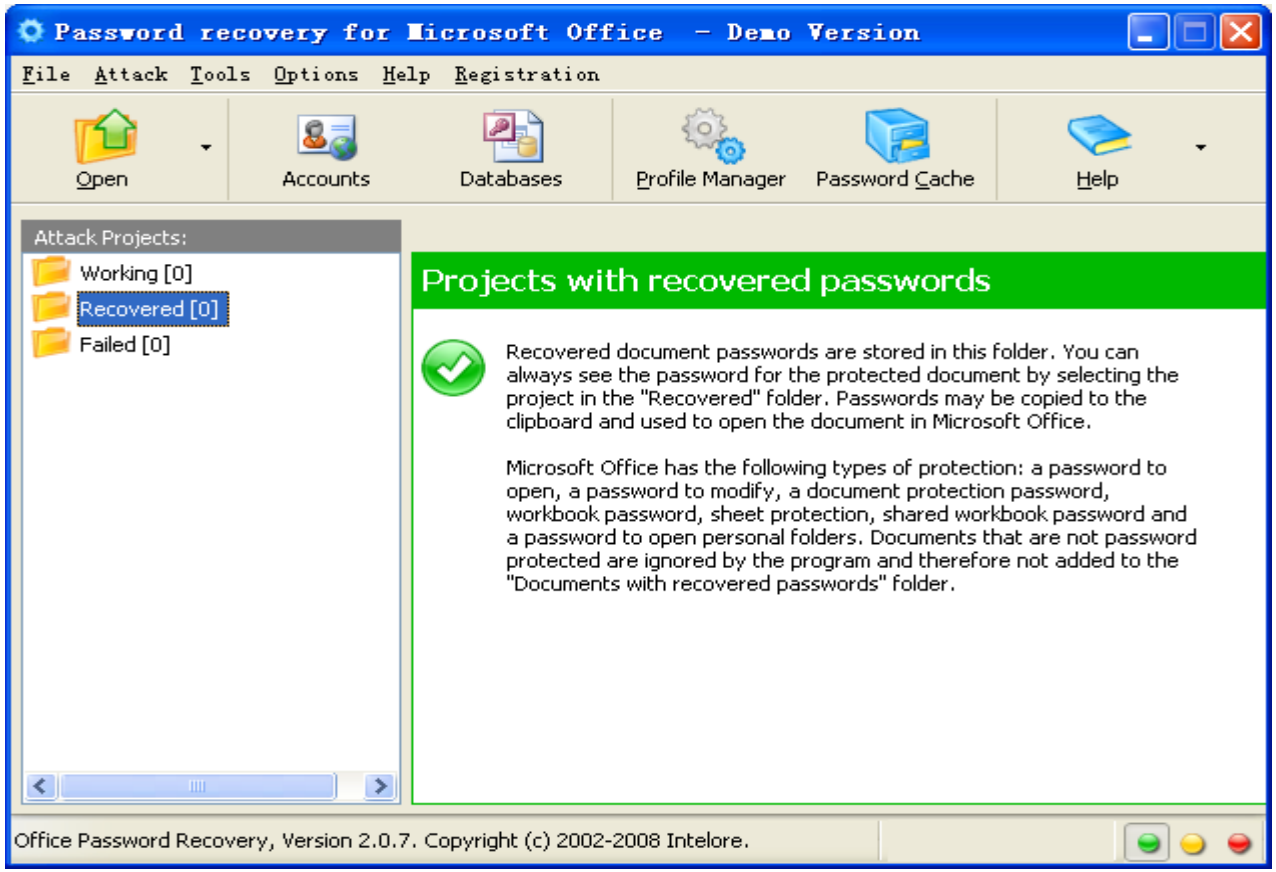
Password Recovery For Microsoft ACCESS



§8.4 密码破解攻击

- 破解各种Office文档密码——工具软件

Password Recovery For Microsoft Office



§8.5 缓冲区溢出攻击

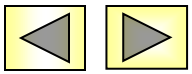
- 缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统当机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。
- 缓冲区溢出的原理是通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

§8.5 缓冲区溢出攻击

- 例如：void function(char *str)

```
{
    char buffer[16];
    strcpy(buffer, str);
}
```

strcpy()直接把str的内容copy到buffer中。这样只要str的长度大于16，就会造成buffer的溢出，使程序运行出错。存在象strcpy这样的问题的标准函数还有strcat()、sprintf()、vsprintf()、gets()、scanf()等。



§8.5 缓冲区溢出攻击

- 缓冲区溢出攻击之所以成为一种常见的安全攻击手段，其原因在于缓冲区溢出漏洞太普遍了，并且攻击易于实现。而且，缓冲区溢出成为远程攻击的主要手段其原因在于缓冲区溢出漏洞给予了攻击者他所想要的一切：植入并且执行攻击代码。被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而得到被攻击主机的控制权。

§8.5 缓冲区溢出攻击

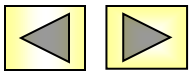
- RPC溢出漏洞
  - Remote Procedure Call(RPC)是Windows操作系统使用的一种远程过程调用协议，RPC协议提供一种进程间的交互通信机制，它允许本地机器上的程序进程无缝的在远程系统中运行代码。该协议的前身是OSF RPC协议，但是增加了微软自己的一些扩展。
- RPC溢出漏洞起因
  - RPC的DCOM接口负责处理DCOM对象激活请求，但不能正确处理畸形消息。
  - 其本质就是对其参数未能进行有效检查。

§8.5 缓冲区溢出攻击

- RPC溢出漏洞的防护方法

（1）在防火墙上封堵相关端口

- 135/UDP;137/UDP; 138/UDP; 139/TCP; 445/TCP;593/TCP
- 在受影响主机禁用COM Internet服务和RPC over HTTP
- 这些端口用于启动与远程计算机的RPC 连接
- 在防火墙上封堵这些端口，可以帮助防火墙内的系统防范通过利用此漏洞进行的攻击
- 缺点：系统不能利用RPC的这些端口进行远程通信



§8.5 缓冲区溢出攻击

- RPC溢出漏洞的防护方法

（1）在防火墙上封堵相关端口

（2）禁用所有受影响的计算机上的DCOM

- 如果一台计算机是一个网络的一部分，则该计算机上的COM 对象将能够通过DCOM 网络协议与另一台计算机上的COM 对象进行通信。您可以禁用特定的计算机上的DCOM，帮助其防范此漏洞
- 缺点：这样做会阻断该计算机上的对象与其他计算机上的对象之间的所有通信
- 如果禁用远程计算机上的DCOM，此后将无法远程访问该计算机来重启DCOM，而只能本地操作该计算机

§8.5 缓冲区溢出攻击

- RPC溢出漏洞的防护方法

（1）在防火墙上封堵相关端口

（2）禁用所有受影响的计算机上的DCOM

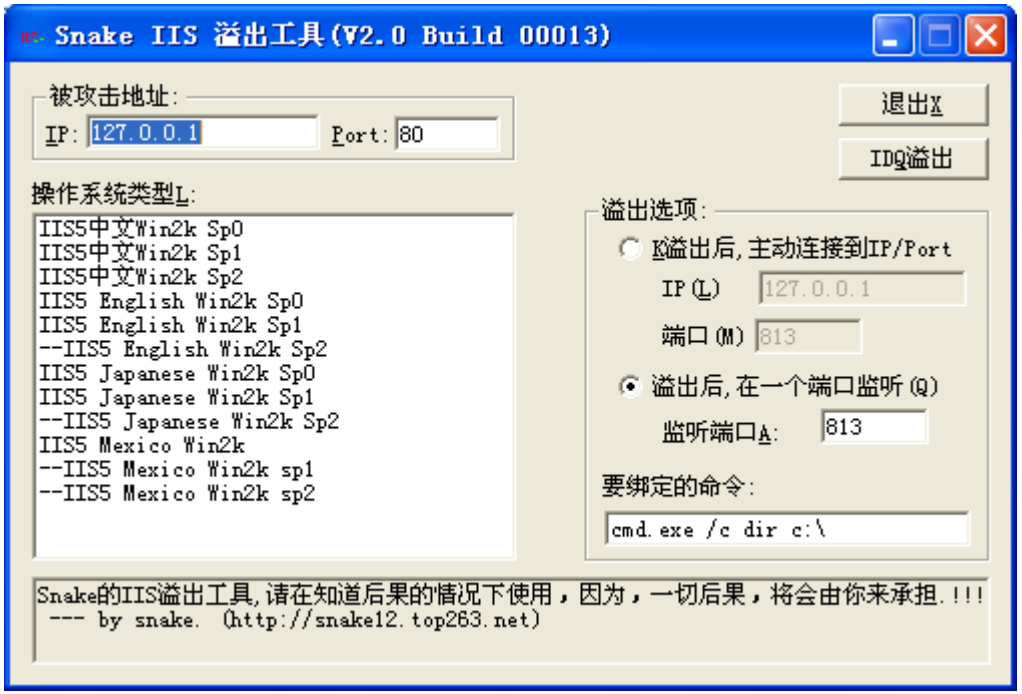
（3）打补丁

- 目前，最好的解决办法是下载微软发布的安全补丁程序

§8.5 缓冲区溢出攻击

IIS溢出攻击

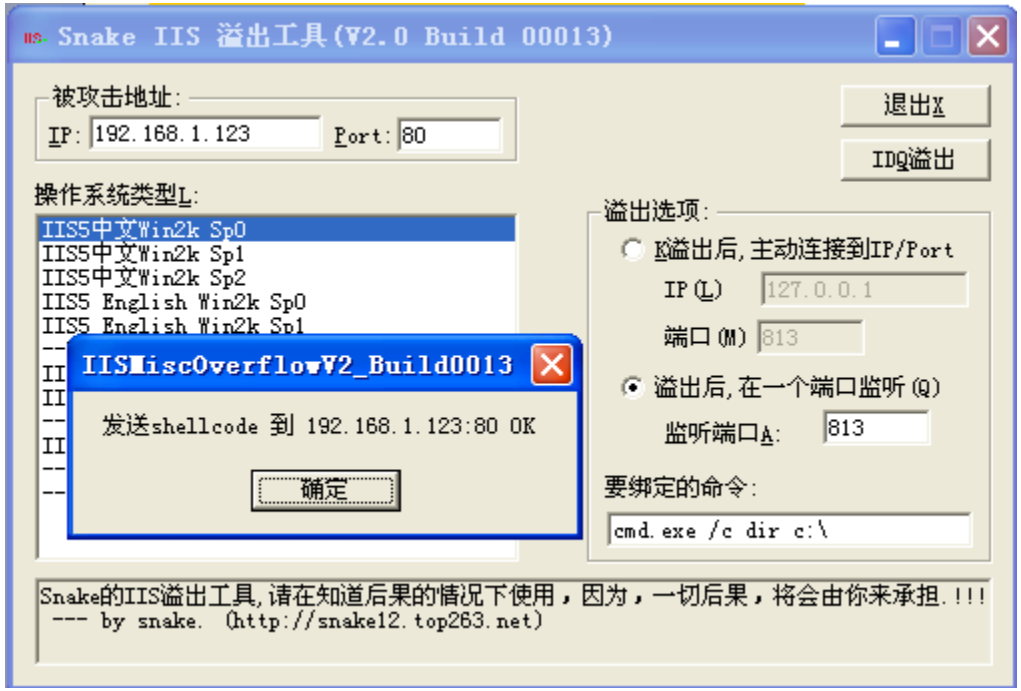
- 利用软件Snake IIS溢出工具可以让对方的IIS溢出，还可以捆绑执行的命令和在对方计算机上开辟端口
- 主界面



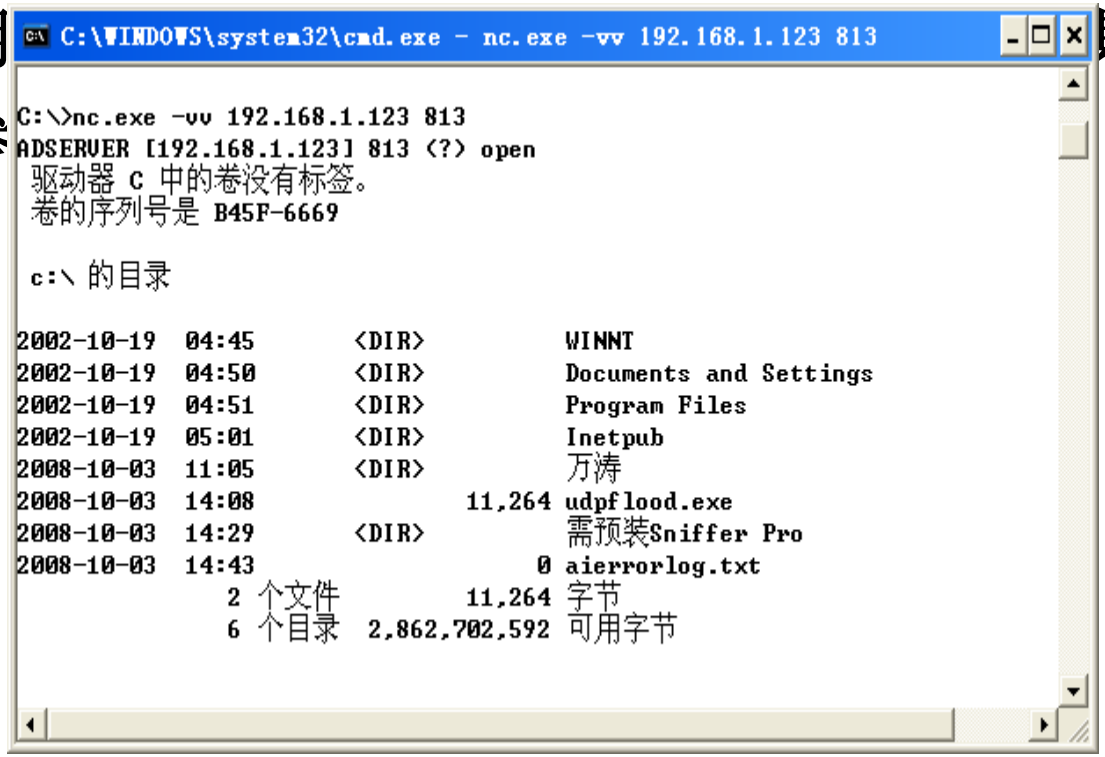
§8.5 缓冲区溢出攻击

IIS溢出攻击

- 攻击完毕后，开辟一个813端口，并在对方计算机上执行命令“dir c:\”，点击“IDQ溢出”，出现攻击成功提示

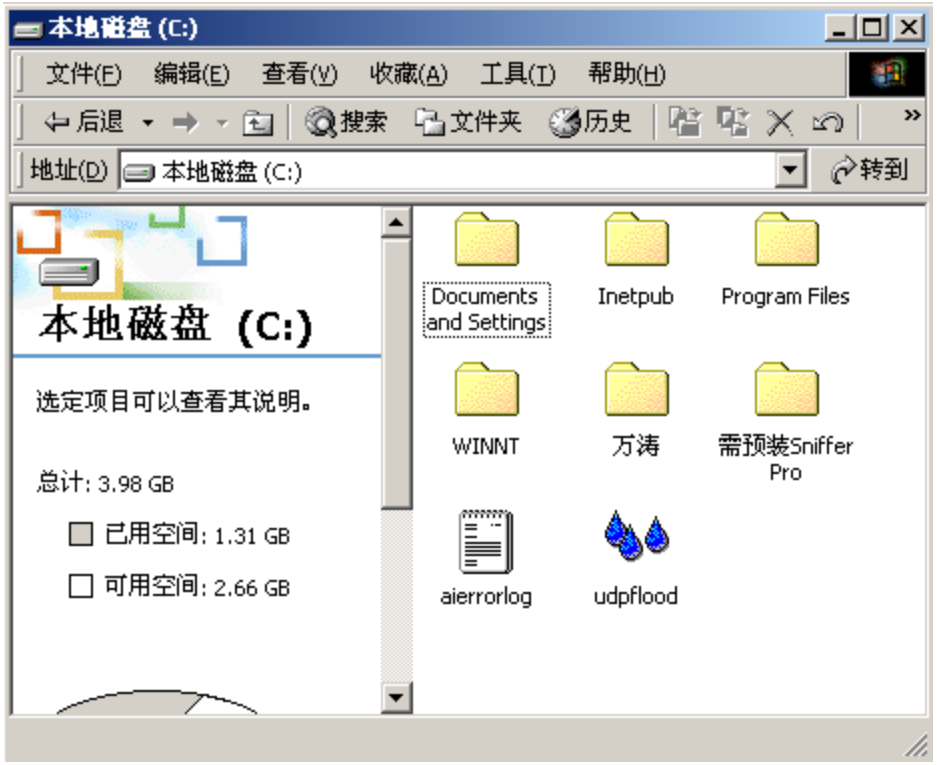


§8.5 缓冲区溢出攻击

- IIS溢出攻击
  - 此时813端口已经开放，利用工具软件nc.exe连接到该端口，将会自动执行刚才发送的DOS命令“dir c:\”
  - 使用其中-vv是程序的参

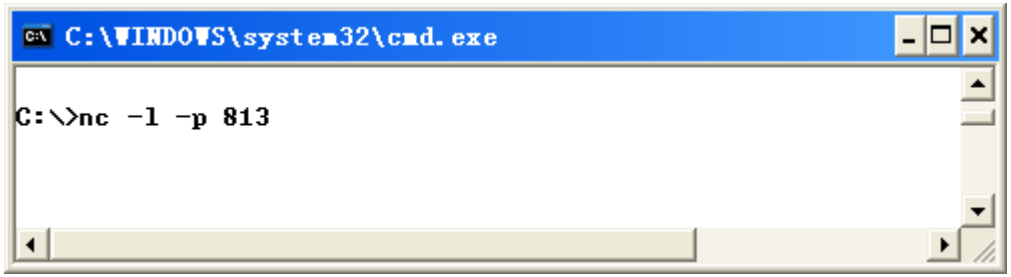
§8.5 缓冲区溢出攻击

- IIS溢出攻击



§8.5 缓冲区溢出攻击

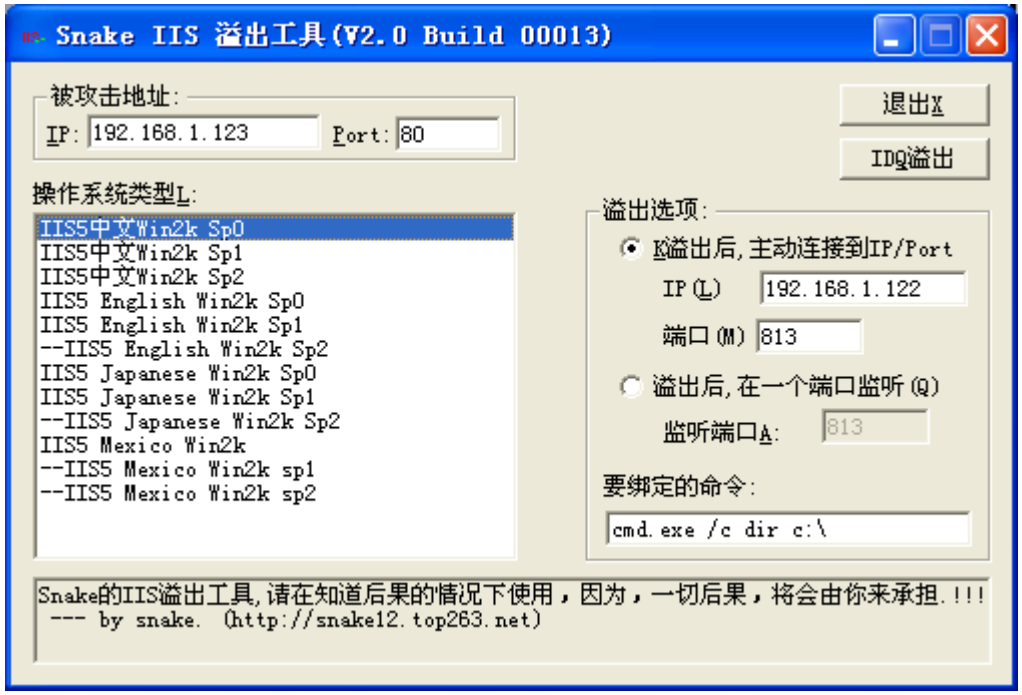
- 本地端口监听
  - 利用nc.exe监听本地的813端口，使用命令“nc -l -p 813”，窗口一直保留



§8.5 缓冲区溢出攻击

➢ 本地端口监听

- 启动工具软件snake，设置本地的IP地址，要攻击的计算机的IP地址，端口是813，然后，点击按钮“IDQ溢出”





§8.5 缓冲区溢出攻击

- 本地端口监听
  - 查看nc命令的DOS框，在该界面下，已经执行了设置的DOS命令。将对方计算机的C盘根目录列出来



§8.6 拒绝服务攻击

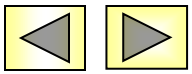
- 拒绝服务攻击，简称DoS（Denial of Service）攻击。
- DoS攻击通过抢占目标主机系统资源使系统过载或崩溃，破坏和拒绝合法用户对网络、服务器等资源的访问，达到阻止合法用户使用系统的目的，是常用的一种攻击方式。
- DoS属于破坏型攻击。它对目标系统本身的破坏性并不是很大，但影响了正常的工作和生活秩序，间接损失严重，社会效应恶劣。
- 凡是造成目标计算机拒绝提供服务的攻击都称为DoS攻击。
- DoS可能由网络部件的物理损坏引起，也可能由网络负荷超载所引起，还可能由不正确的使用网络协议而引起。

§8.6 拒绝服务攻击

- DoS攻击的两种基本形式
  - 计算机网络带宽攻击。以极大的通信量冲击网络，使网络所有可用的带宽都被消耗掉，最后导致合法用户的请求无法通过。
  - 连通性攻击。用大量的连接请求冲击计算机，最终导致计算机无法再处理合法用户的请求。
- DoS攻击发生时的特点
  - 消耗系统或网络资源，使系统过载或崩溃。
  - 难以辨别真假。
  - 使用不应存在的非法数据包来达到拒绝服务攻击的目的。
  - 有大量的数据包来自相同的源。

§8.6 拒绝服务攻击

- DoS 攻击类型
  - SYN flood
  - Smurf
  - land
  - Ping of death
  - UDP Flood
  - teardrop



§8.6 拒绝服务攻击

- SYN flood（同步风暴）攻击
  - 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的攻击方式。
  - TCP是基于连接的，为了在服务端和客户端之间传送TCP数据，必须先建立TCP连接。建立TCP连接的标准过程：
    - 请求端发送一个包含SYN标志的TCP报文，同步报文会指明客户端使用的端口以及TCP连接的初始序号
    - 服务器收到SYN报文后，返回一个SYN+ACK的报文，表示客户端的请求被接受，同时TCP序号被加1
    - 客户端也返回一个ACK给服务器端，同样TCP序列号被加1

§8.6 拒绝服务攻击

- SYN flood（同步风暴）攻击
  - 假设一个用户向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN+ACK应答报文后是无法收到客户端的ACK报文的。在这种情况下服务器端会重试，再次发送SYN+ACK给客户端，并等待一段时间，判定无法建立连接后，丢弃这个未完成的连接。这段等待时间称为SYN中止时间（Timeout），一般为30秒～2分钟。
  - 如果攻击者大量模拟这种情况，服务器端为了维护非常大的半连接列表就会消耗非常多的资源。此时从正常客户的角度来看，服务器已经丧失了对正常访问的响应，这便是SYN Flood攻击的机理。

§8.6 拒绝服务攻击

- SYN flood（同步风暴）攻击



§8.6 拒绝服务攻击

- SYN flood（同步风暴）攻击

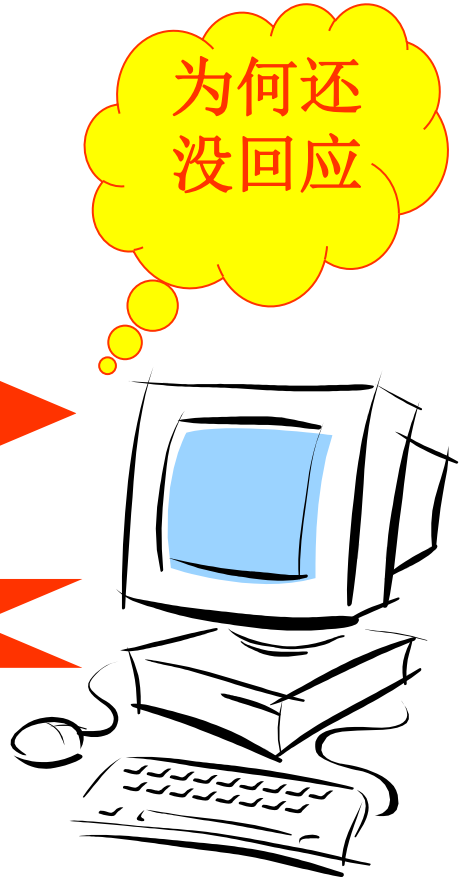


伪造地址进行SYN请求

SYN （我可以连接吗？）

ACK （可以）/SYN（请确认！）

？ ？ ？



攻击者

不能建立正常的连接
其它正常用户得不到响应

受害者

§8.6 拒绝服务攻击

- SYN flood（同步风暴）攻击



攻击者

大量的tcp connect

正常tcp connect

正常tcp connect

正常tcp connect

正常tcp connect



正常用户

正常tcp connect

不能建立正常的连接

这么多需要处理？



受害者

§8.6 拒绝服务攻击

- 针对SYN flood攻击的防范措施
  - 优化系统配置
  - 优化路由器配置
  - 完善基础设施
  - 使用防火墙
  - 主动监视

缩短超时时间，增加板连接队列

配置路由器的外网卡，丢弃那些

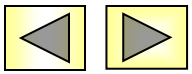
现有的网络体系结构没有对源IP

采用半透明网关技术的防火墙能有效防范SYN flood攻击

而且许多攻击手段都是利用现有网络协议的缺陷。因此对整个网络体系结构的再改造十分重要。

§8.6 拒绝服务攻击

- Smurf攻击
  - 该攻击向一个子网的广播地址发一组ICMP回应请求数据包,并且将源地址伪装成想要攻击的主机地址。子网中所有主机都将向被伪装的源地址发回ICMP回应应答。
  - 攻击者通过几百个数据包就可以产生成千上万的数据包，这样不仅可以造成目标主机的拒绝服务，而且还会使目标子网的网络本身也遭到DoS攻击。

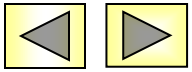


§8.6 拒绝服务攻击

- Land攻击
  - IP协议中IP源地址和目标地址相同
  - 操作系统如Window NT不知道该如何处理这种情况，就可能造成死机。
  - Land攻击向UDP目标端口135发送伪装的RPC的UDP数据包，使之看上去像一个RPC服务器在向另一个RPC服务器发送数据，目标服务器将返回一个REJECT数据包，而源服务器用另一个REJECT数据包应答，结果就会造成死循环，只有当数据包作为异常处理被丢掉时循环才会中止。
  - 如果将伪装的UDP数据包发送至多台主机，就会产生多个循环，将消耗大量处理器资源和网络带宽。

§8.6 拒绝服务攻击

- Ping of death攻击
  - 根据有关IP协议规定的RFC791，占有16位的总长度控制字确定了IP包的总长度为65535字节，其中包括IP数据包的包头长度。
  - Ping to death攻击发送超大尺寸的ICMP数据包，使得封装该ICMP数据包的IP数据包大于65535字节，目标主机无法重新组装这种数据包分片，可能造成缓冲区溢出、系统崩溃。

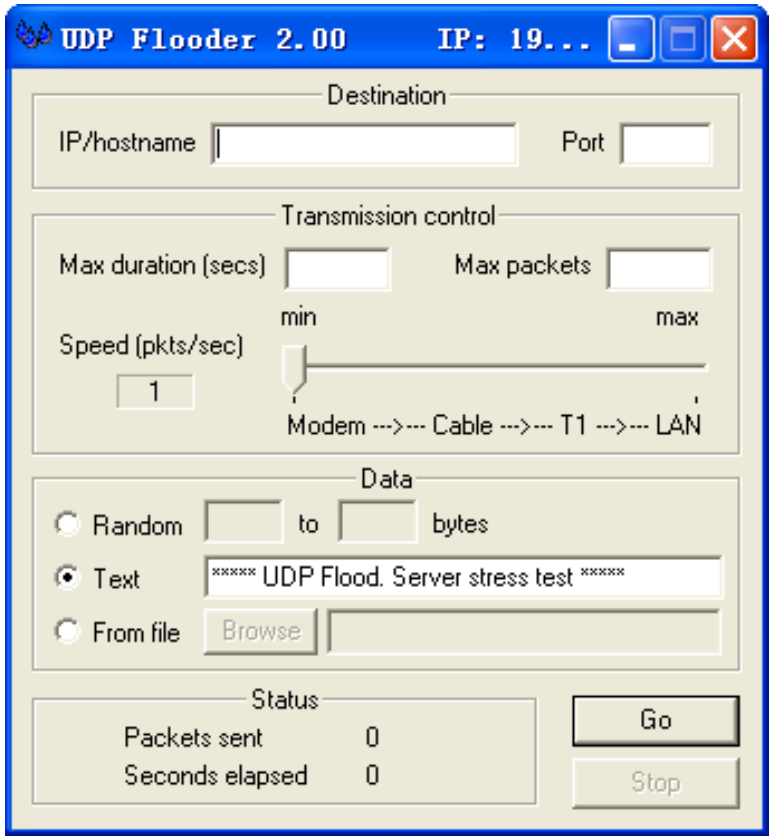


§8.6 拒绝服务攻击

- UDP Flood攻击
  - 用Chargen和Echo来传送毫无用处的数据来占用所有的带宽。在攻击过程中，通过伪造与某一主机的hargen服务之间的一次UDP连接，回复地址指向开着Echo服务的一台主机，这样就生成在两台主机之间的足够多的无用数据流，如果足够多的数据流就会导致针对带宽消耗的拒绝服务攻击。
  - 杜绝UDP Flood攻击的最好办法是关掉不必要的TCP/IP服务，或者配置防火墙以阻断来自Internet的UDP服务请求，不过这可能会阻断一些正常的UDP服务请求。

§8.6 拒绝服务攻击

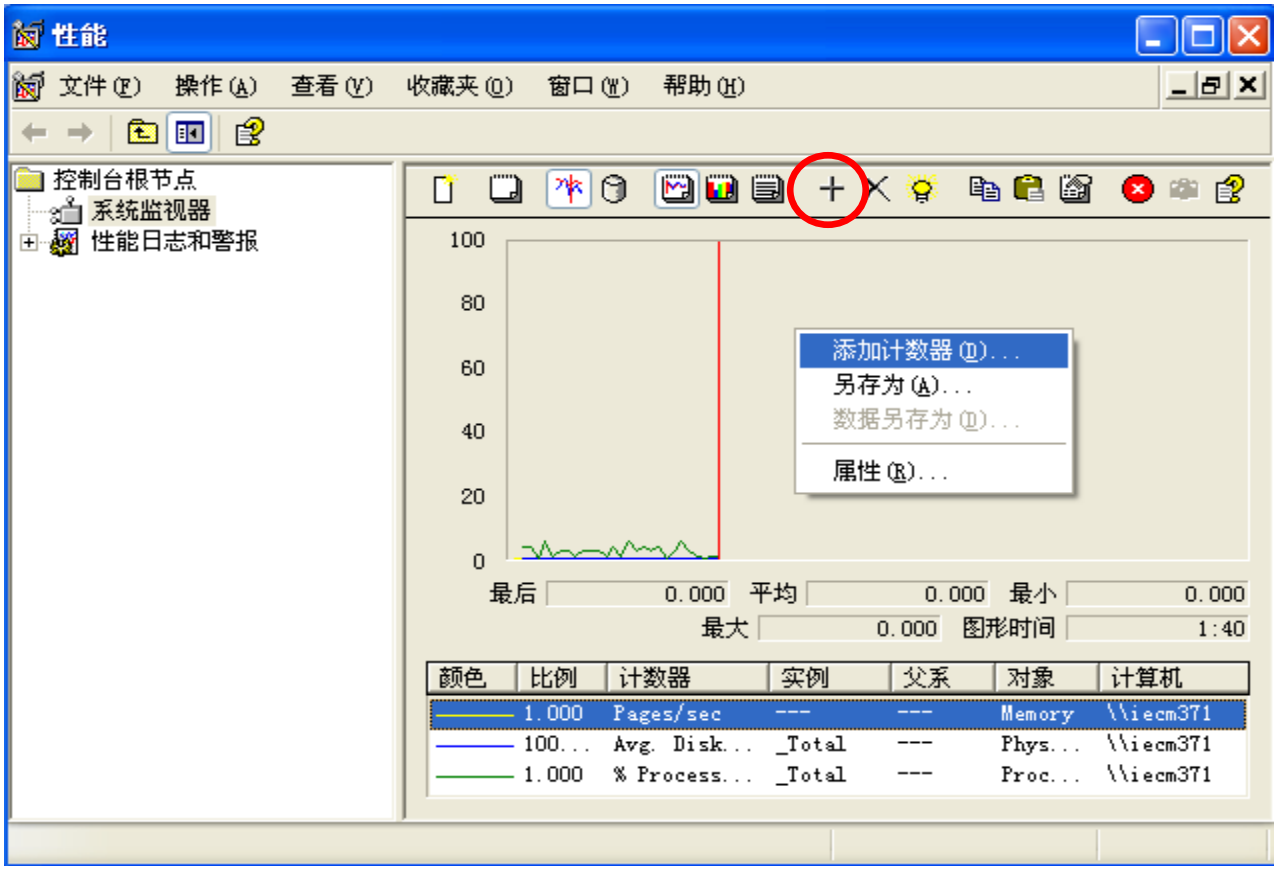
- UDP Flood攻击——工具软件UDP Flooder
  - 一种采用UDP-Flood攻击方式的DoS软件，它可以向特定的IP地址和端口发送UDP包



§8.6 拒绝服务攻击

- UDP Flood攻击——工具软件UDP Flooder

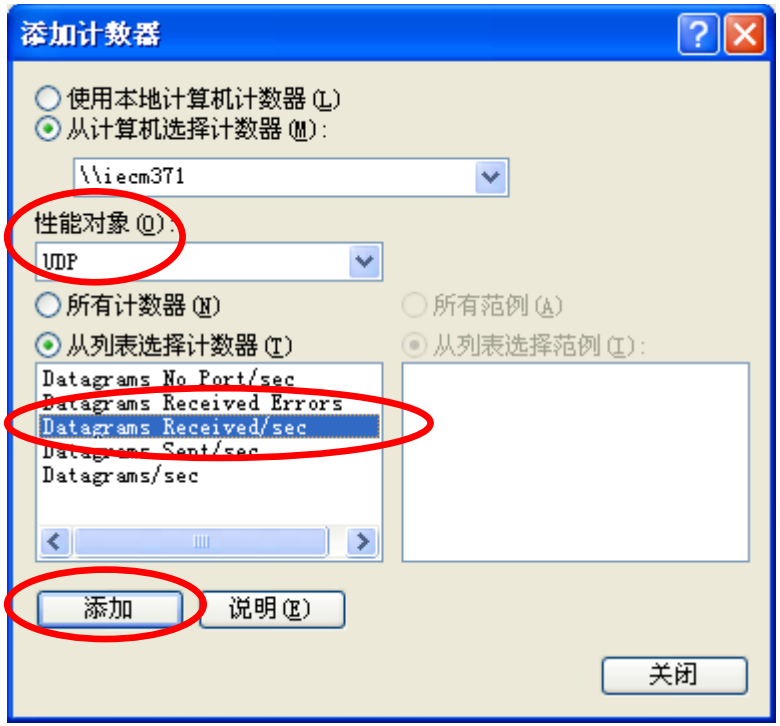
  控制面板→管理工具→性能



§8.6 拒绝服务攻击

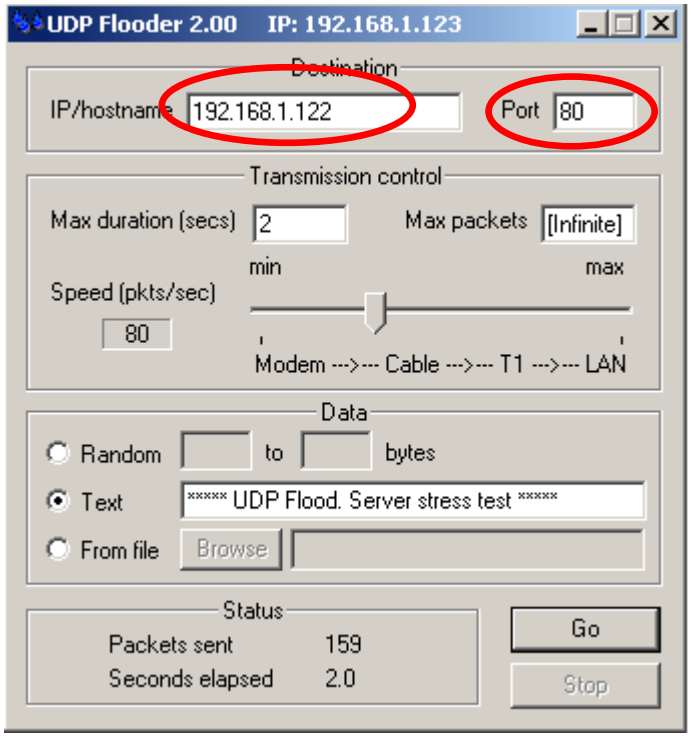
- UDP Flood攻击——工具软件UDP Flooder

在“性能对象”框中选择UDP协议，在“从列表选择计数器”中，选择“Datagram Received/Sec”即对收到的UDP数据包进行计数，添加对UDP数据包的计数器



§8.6 拒绝服务攻击

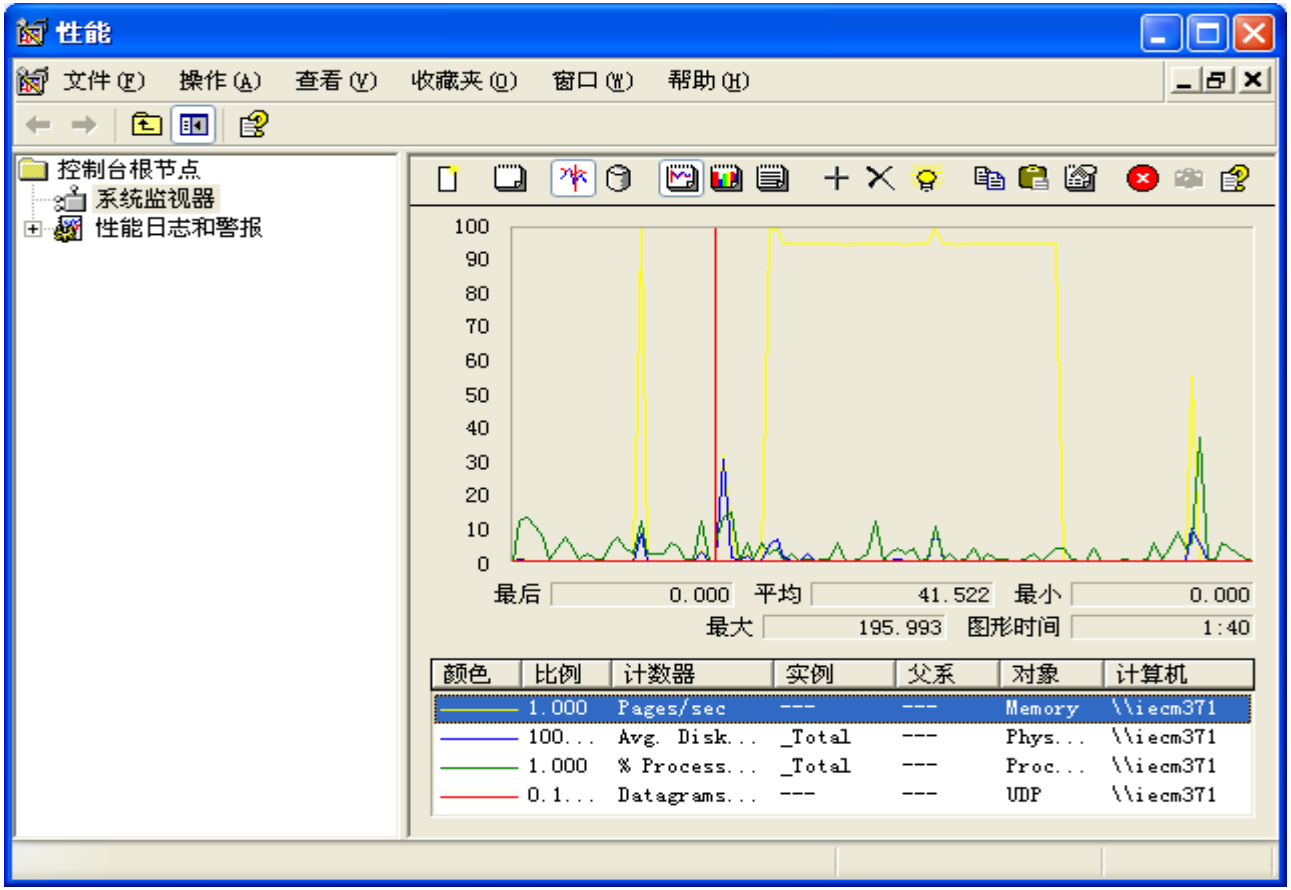
- UDP Flood攻击——工具软件UDP Flooder



§8.6 拒绝服务攻击

- UDP Flood攻击——工具软件UDP Flooder

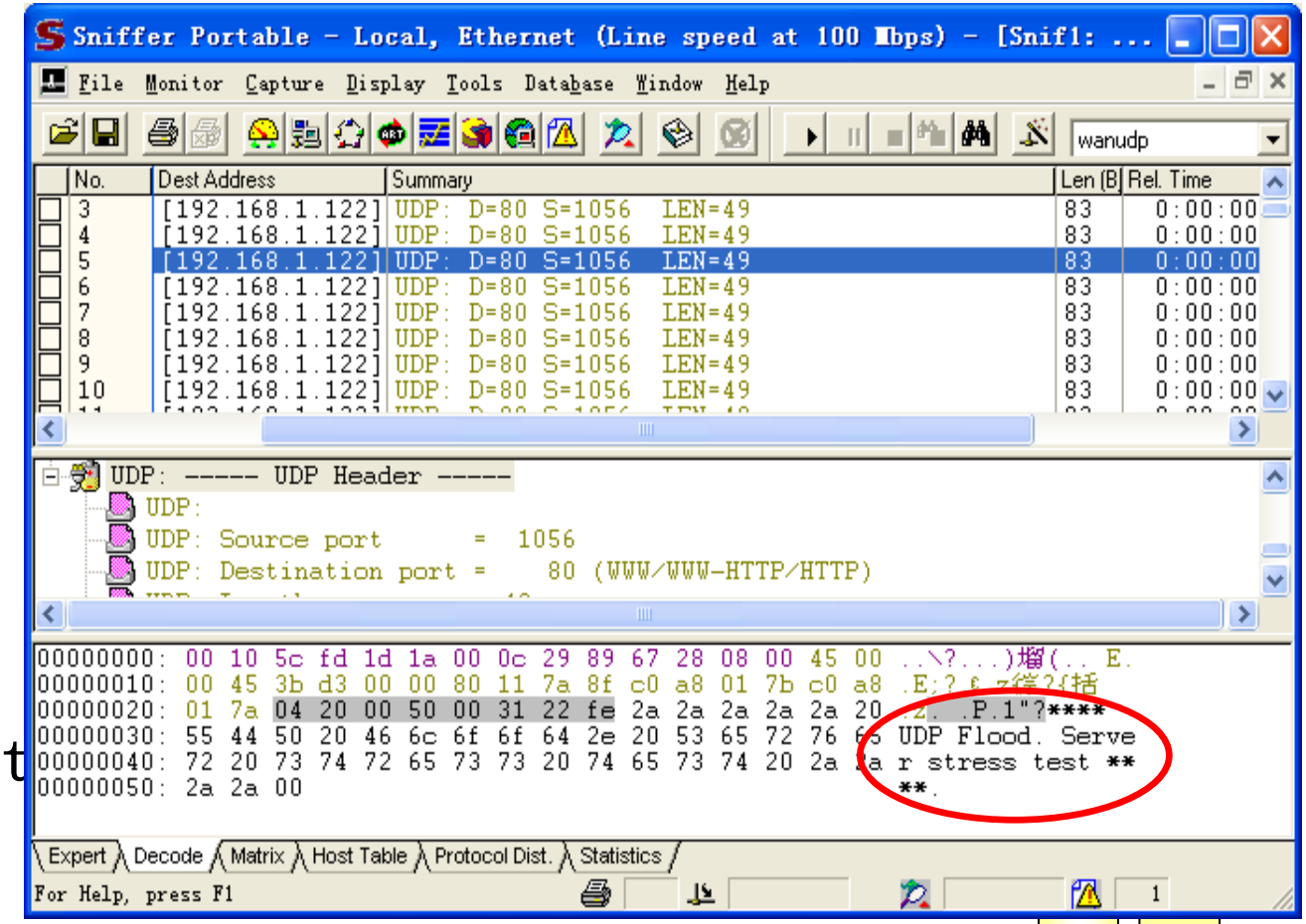
系统监视器对UDP的监测图



§8.6 拒绝服务攻击

- UDP Flood攻击——工具软件UDP Flooder

在被攻击的计算机上打开sniffer pro，可以捕捉UDP数据包，看到大量内容为“UDP Flood. Server stresst的UDP数据包



§8.6 拒绝服务攻击

- Teardrop（泪滴）攻击
  - 它利用的是系统在实现时的一个错误，即攻击特定的IP协议栈实现片段重组代码存在的缺陷。当网络分组穿越不同的网络时，有时候需要根据网络最大传输单元MTU来把它们分割成较小的片，早期的Linux系统在处理IP分片重组问题时，尽管对片段是否过长进行检查，但对过短的片段却没有进行验证，所以导致了泪滴形式的攻击，会造成系统的死机或重新启动
  - 防御泪滴攻击的最好办法是升级服务包软件，如下载操作系统补丁或升级操作系统等。另外，在设置防火墙时对分组进行重组而不进行转发，也可以防止这种攻击。

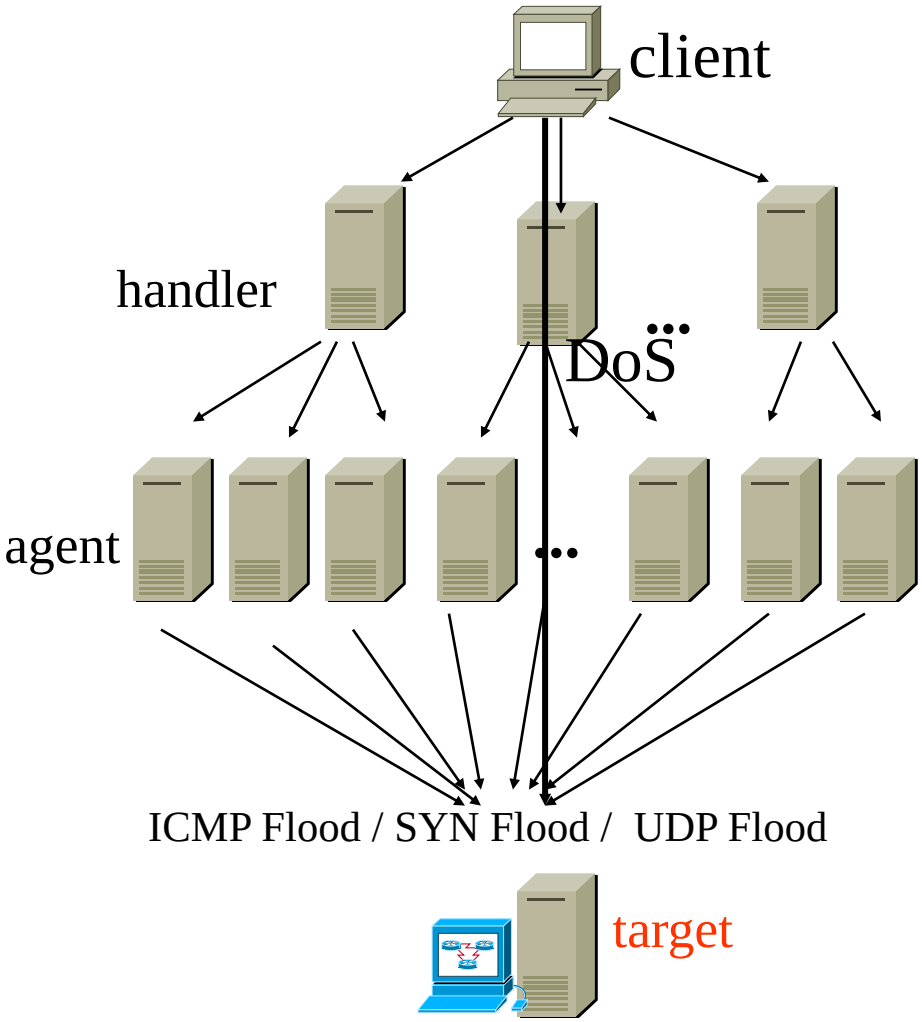
§8.6 拒绝服务攻击

- 分布式拒绝服务攻击，简称DDoS（Distributed Denial of Service）攻击。
- 一种基于DoS的特殊形式的拒绝服务攻击。
- 攻击者将多台受控制的计算机联合起来向目标计算机发起DoS攻击，它是一种大规模协作的攻击方式，主要瞄准比较大的商业站点，具有较大的破坏性

§8.6 拒绝服务攻击

- DDoS攻击网络结构
  - DDoS攻击由攻击者、主控端（master）、代理端(zombie)三部分组成，三者在攻击中扮演不同的角色。
  - 攻击者是整个DDoS攻击发起的源头，它事先已经取得了多台主控端计算机的控制权
  - 主控端计算机分别控制着多台代理端计算机。在主控端计算机上运行着特殊的控制进程，可以接收攻击者发来的控制指令，操作代理端计算机对目标计算机发起DDoS攻击。

§8.6 拒绝服务攻击


client
handler
DoS
agent
ICMP Flood / SYN Flood / UDP Flood
target

§8.6 拒绝服务攻击

- DDoS的攻击步骤
  - 黑客使用扫描工具探测扫描大量主机寻找潜在入侵目标。
  - 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。
  - 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。
  - 黑客发送控制命令给主机，准备启动对目标系统的攻击
  - 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。
  - 目标系统被无数的伪造的请求所淹没，从而无法对合法用户进行响应，DDOS攻击成功。

§8.6 拒绝服务攻击

- DDoS攻击的防范
  - 增强系统安全性，例如加固系统用户和口令的安全性；及早发现系统存在的攻击漏洞，及时安装系统补丁程序；禁止所有不必要的服务；周期性的对系统进行安全性审核等。
  - 利用防火墙、路由器等网络和网络安全设备加固网络的安全性，如禁止对主机非开放服务的连接、限制同时打开的SYN半连接数量、严格限制服务程序的对外访问请求等。
  - 强化路由器等网络设备的访问控制功能，配置好访问控制列表的过滤规则，禁止网络不用的UDP和ICMP包通过。

§8.6 拒绝服务攻击

- DDoS攻击的防范
  - 加强与ISP的合作，当发现攻击现象时，与ISP协商实施严格的路由访问控制策略，以保护带宽资源和内部网络。
  - 采用DDoS监测工具，加强对DDoS攻击的监测，例如DDoSPing、Zombie Zapper和wtrinscan等，它们可以检测具有代表性的攻击，比如Wintrinoo，Stacheldraht 和TFN等。

§8.6 拒绝服务攻击

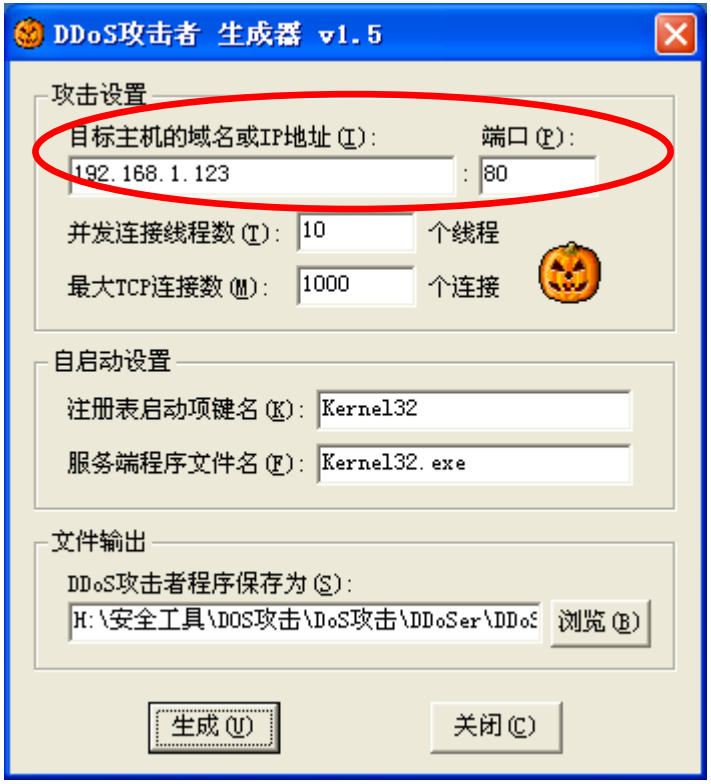
- 对付正在进行的DDOS攻击
  - 首先，检查攻击来源，通常黑客会通过很多假的IP地址发起攻击，此时，用户若能够分辨出哪些是真IP地址，哪些是假IP地址，然后了解这些IP来自哪些网段，再找网段管理员把机器关掉，即可消除攻击。
  - 其次，找出攻击者所经过的路由，把攻击屏蔽掉。若黑客从某些端口发动攻击，用户可把这些端口屏蔽掉，以狙击入侵。
  - 最后一种比较折衷的方法是在路由器上滤掉ICMP。

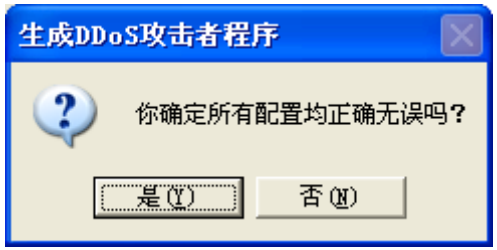
§8.6 拒绝服务攻击

- DDOS攻击——工具DDoSer
  - 软件分为生成器(DDoSMaker.exe)与DDoS攻击者程序(DDoSer.exe)两部分
  - DDoS攻击程序通过生成器DDoSMaker.exe生成。生成时可以自定义一些设置（攻击目标域名或IP地址、端口等）
  - DDoS攻击程序默认的文件名DDoSer.exe，可改名。攻击程序类似木马软件的服务器端程序，程序运行后不会显示任何界面，看上去好象没有反应，其实它已经将自己复制到系统里面了，并且会在每次开机时自动运行，此时可以将拷过去的安装程序删除。
  - DDoSer使用的攻击手段是SYN Flood方式。

§8.6 拒绝服务攻击

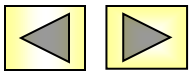
- DDOS攻击——工具DDoSer





§8.6 拒绝服务攻击

- DDOS攻击——工具DDoSer
  - 软件就会自动生成一个DDoSer.exe的可执行文件，这个文件就是攻击程序
  - 运行DDoSer.exe后，这台主机就成了攻击者的代理端，主机会自动发出大量的半连接SYN请求，可以通过netstat命令来查看网络状态

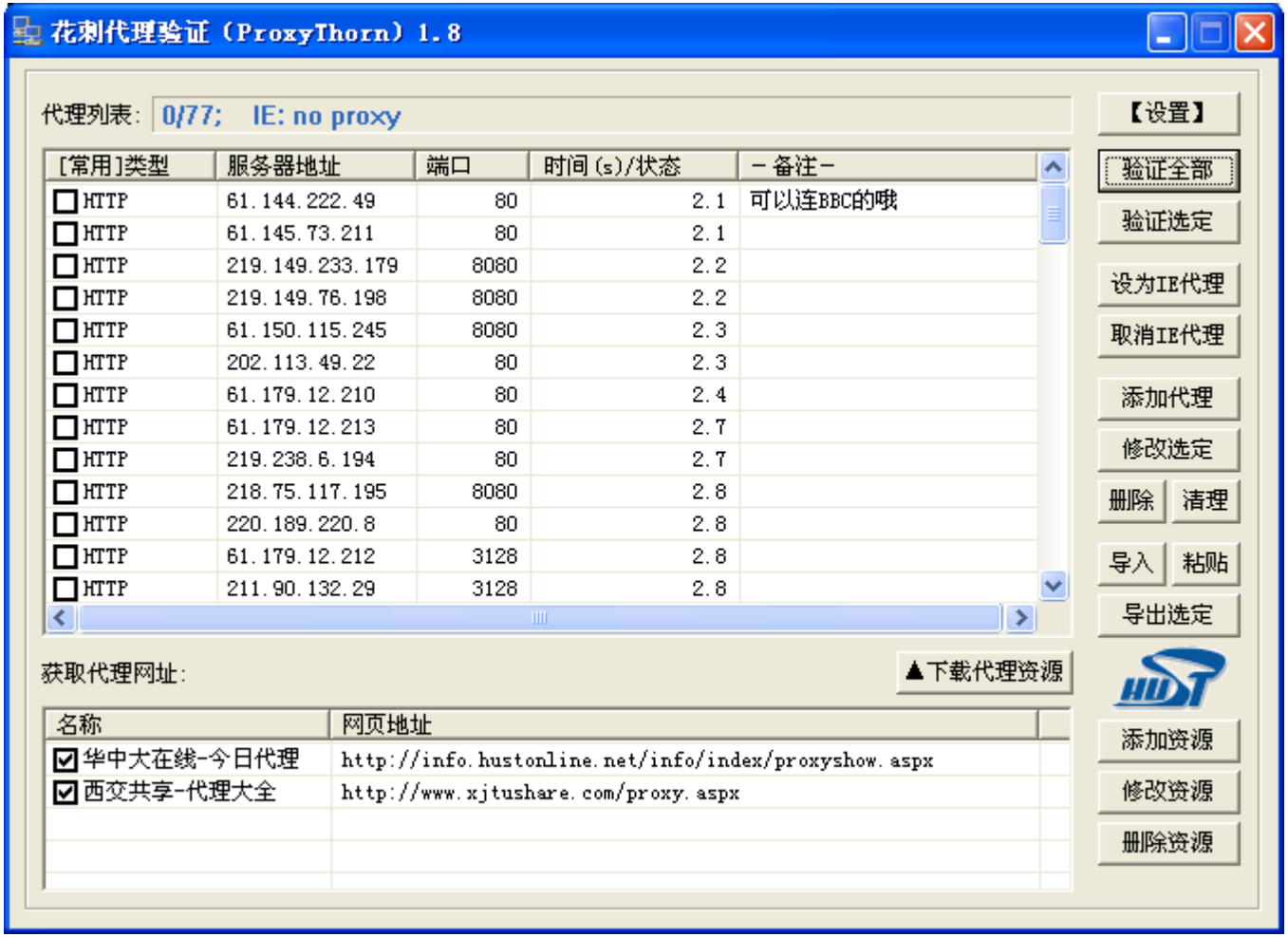


§8.6 拒绝服务攻击

- DDOS攻击——CC攻击
  - CC主要是用来攻击页面的
  - 对于论坛，访问的人越多，论坛的页面越多，数据库就越大，被访问的频率也越高，占用的系统资源也就相当可观
  - CC就是充分利用这个特点，模拟多个用户(多少线程就是多少用户)不停的进行访问(访问那些需要大量数据操作，就是需要大量CPU时间的页面)
  - 代理可以有效地隐藏身份，也可以绕开所有的防火墙，因为几乎所有的防火墙都会检测并发的TCP/IP连接数目，超过一定数目一定频率就会被认为是Connection-Flood

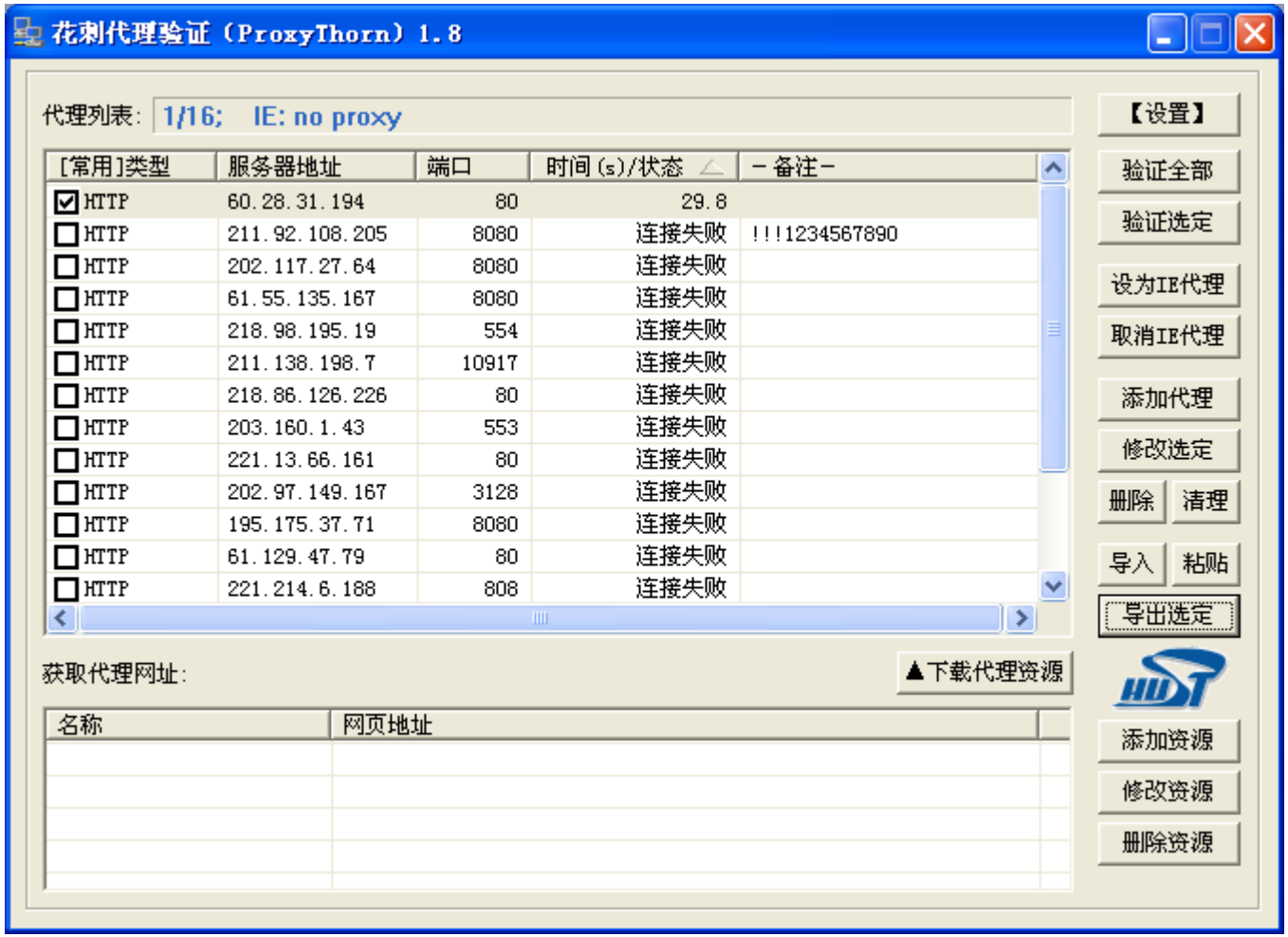
§8.6 拒绝服务攻击

- 代理查找和验证软件——“花刺代理”



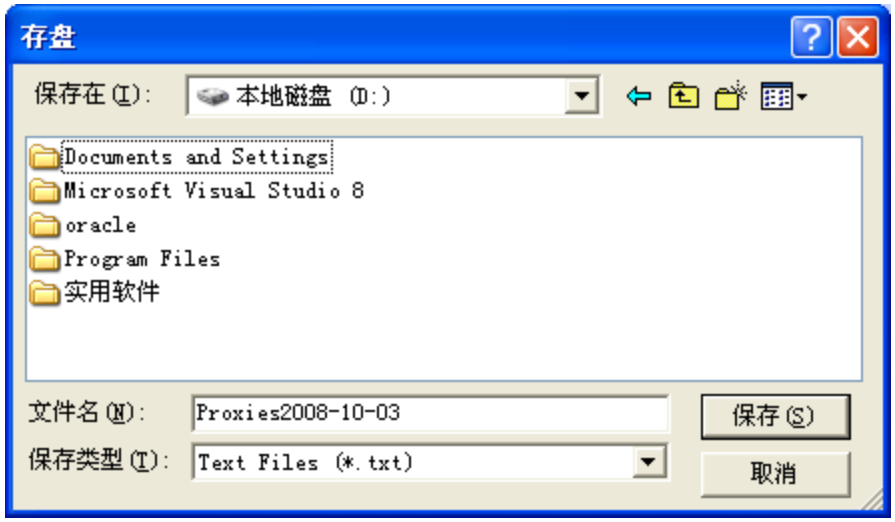
§8.6 拒绝服务攻击

- 代理查找和验证软件——“花刺代理”



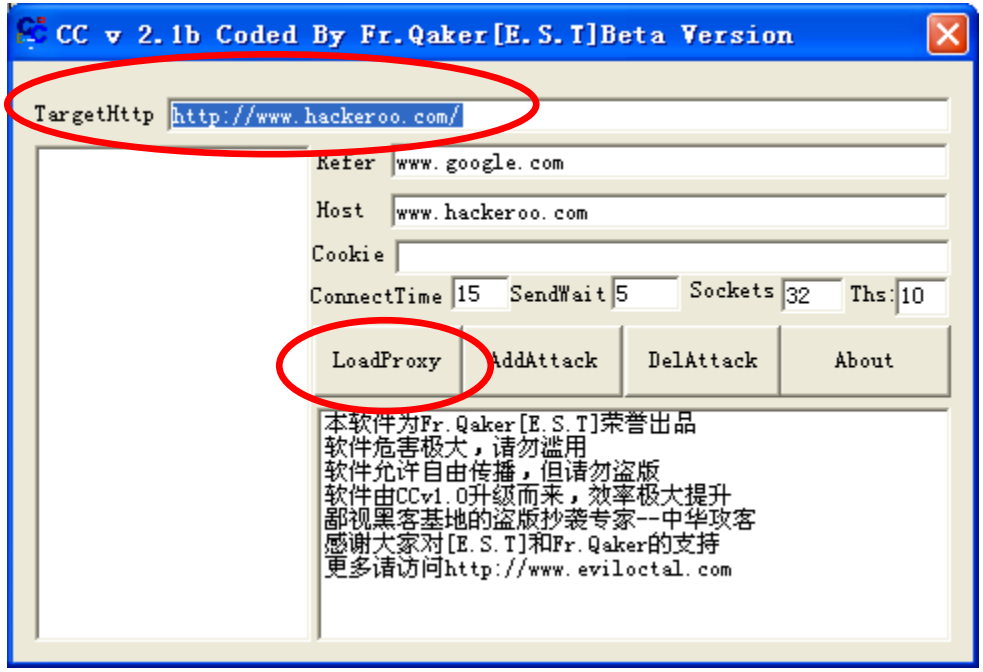
§8.6 拒绝服务攻击

- 代理查找和验证软件——“花刺代理”



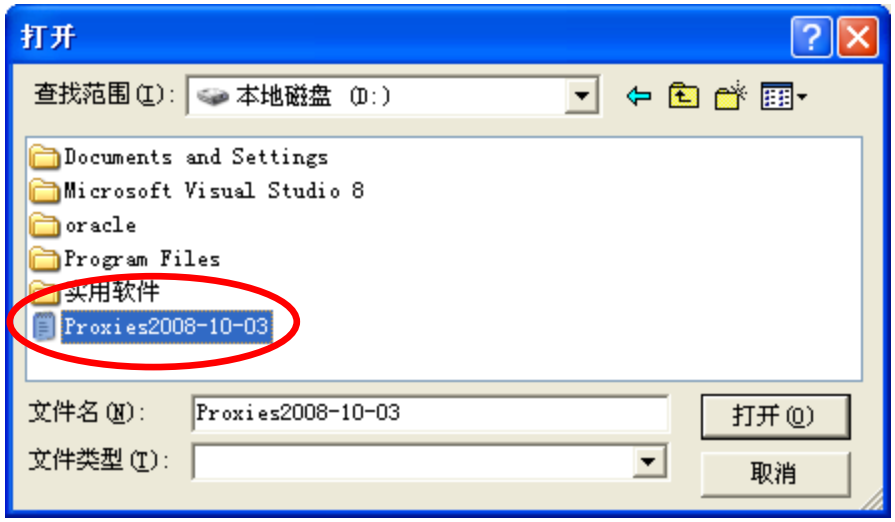
§8.6 拒绝服务攻击

- DDOS攻击——CC攻击



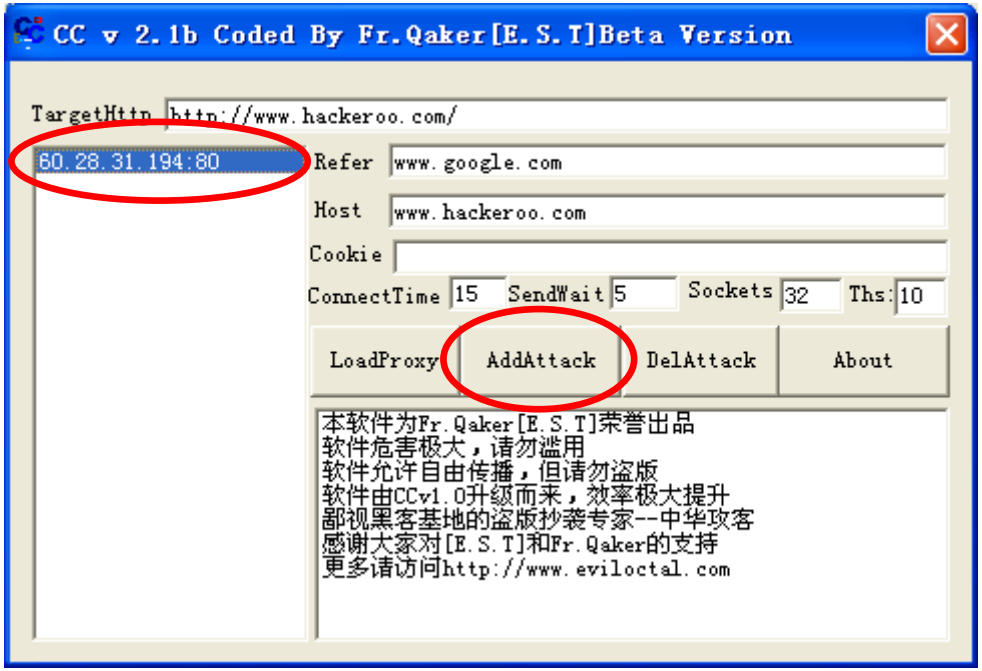
§8.6 拒绝服务攻击

- DDOS攻击——CC攻击



§8.6 拒绝服务攻击

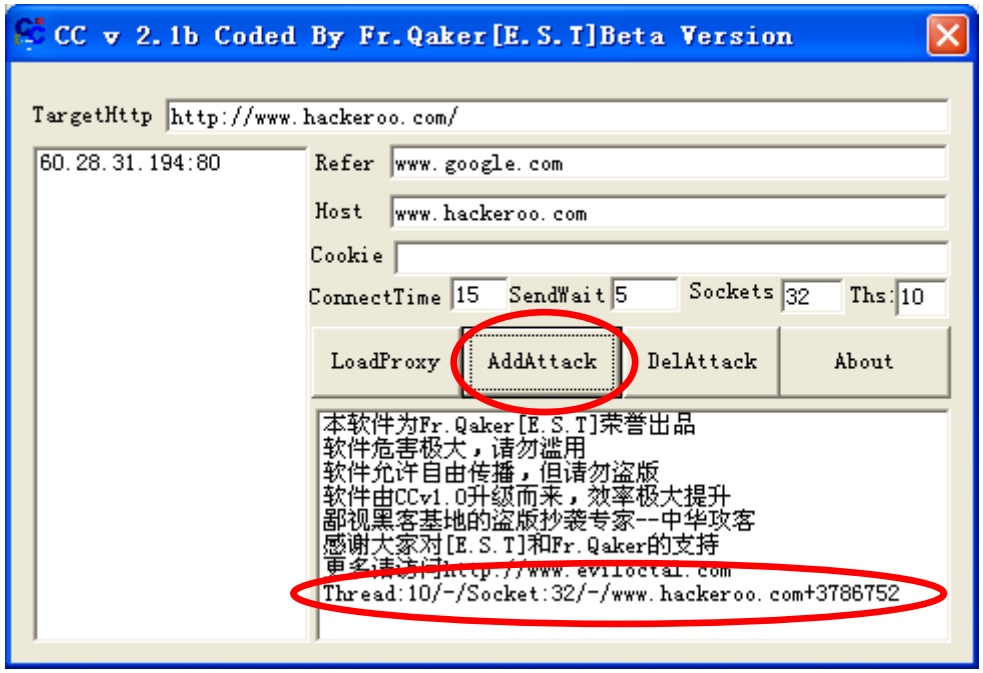
- DDOS攻击——CC攻击





§8.6 拒绝服务攻击

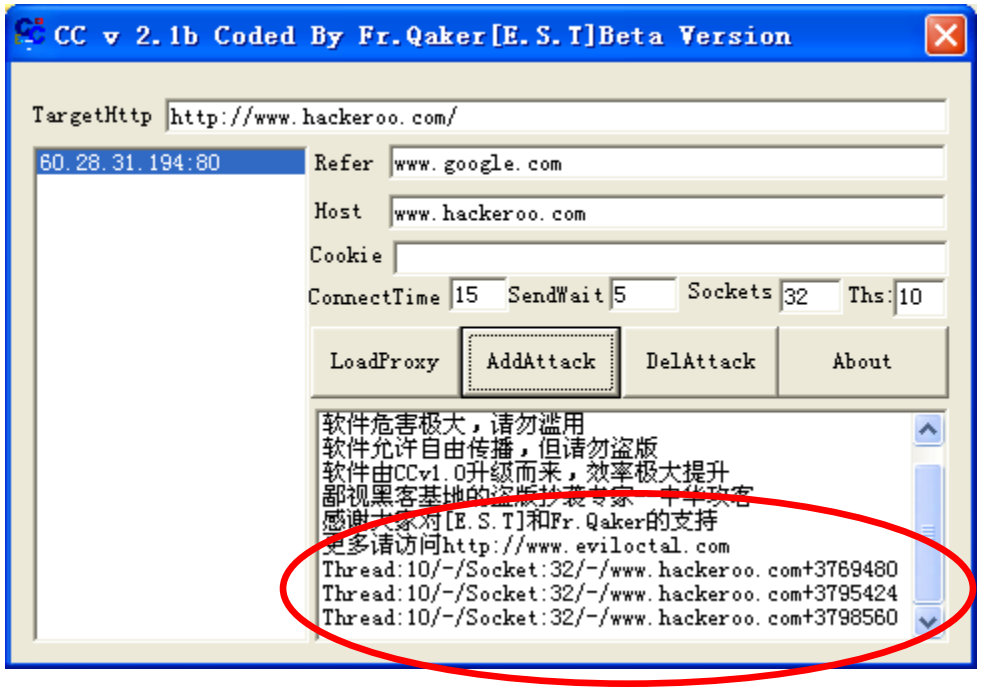
- DDOS攻击——CC攻击





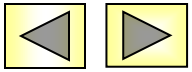
§8.6 拒绝服务攻击

- DDOS攻击——CC攻击



§8.7 网络后门与木马

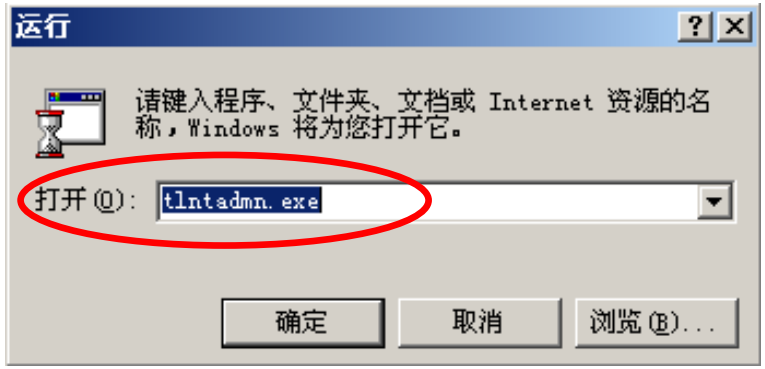
- 为了保持对已经入侵的主机长久的控制，需要在主机上建立网络后门，以后可以直接通过后门入侵系统。
- 网络后门是保持对目标主机长久控制的关键策略。可以通过建立服务端口和克隆管理员帐号来实现。
- 只要能不通过正常登录进入系统的途径都称之为网络后门。
- 后门的好坏取决于被管理员发现的概率。只要是不容易被发现的后门都是好后门。留后门的原理和选间谍是一样的，让管理员看了感觉没有任何特别的。



§8.7 网络后门与木马

一、远程启动Telnet服务

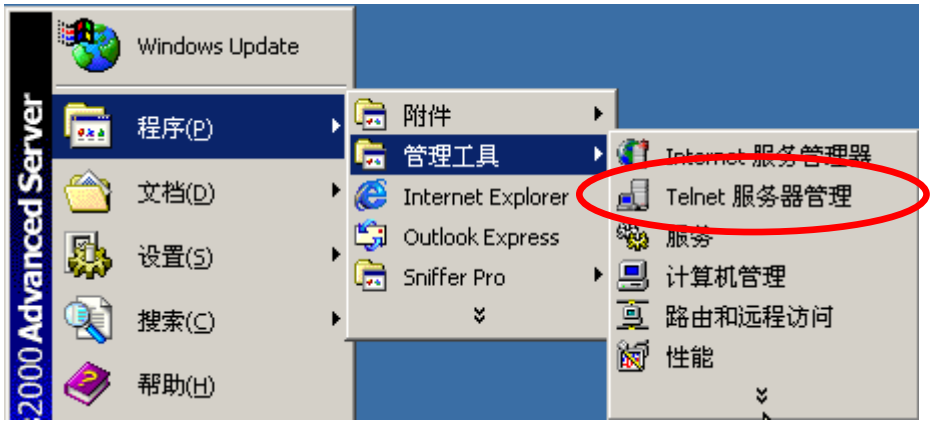
- 利用主机上的Telnet服务，有管理员密码就可以登录到对方的命令行，进而操作对方的文件系统。如果Telnet服务是关闭的，就不能登录了。
- 默认情况下，Windows 2000 Server的Telnet是关闭的
- 启动本地Telnet服务方法一：运行窗口输入tlntadmn.exe命令



§8.7 网络后门与木马

一、远程启动Telnet服务

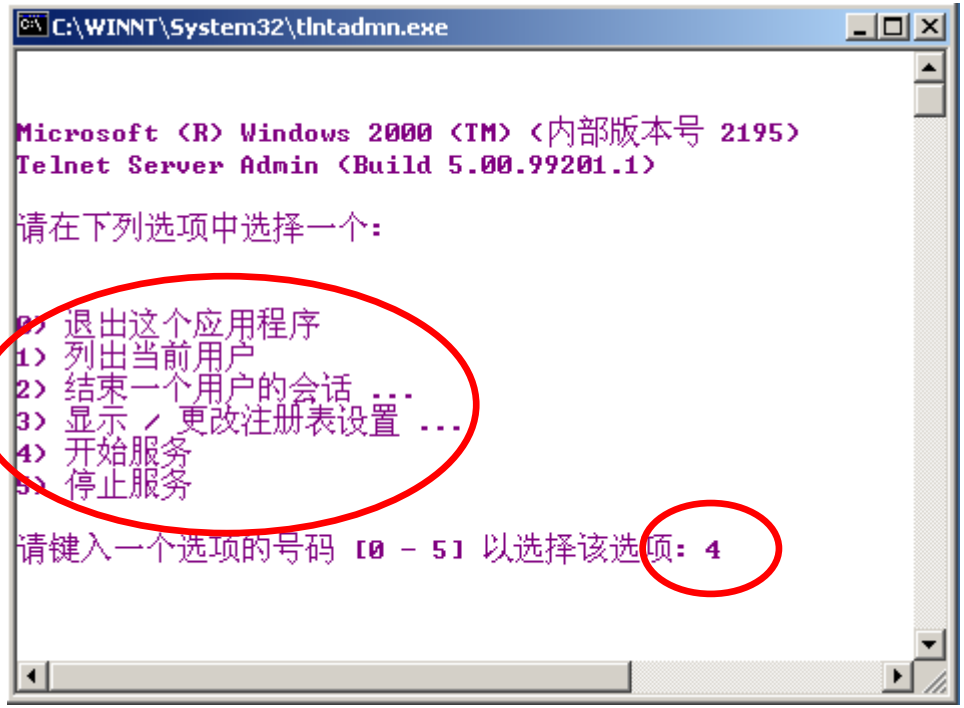
- 利用主机上的Telnet服务，有管理员密码就可以登录到对方的命令行，进而操作对方的文件系统。如果Telnet服务是关闭的，就不能登录了。
- 默认情况下，Windows 2000 Server的Telnet是关闭的
- 启动本地Telnet服务方法二：程序→管理工具→Telnet服务器管理



§8.7 网络后门与木马

➢ 一、远程启动Telnet服务

- 在随后启动的DOS窗口中输入4启动本地Telnet服务

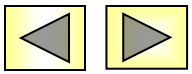


§8.7 网络后门与木马

一、远程启动Telnet服务——工具RTCS.vbe

- 使用该工具需要知道对方具有管理员权限的用户名和密码
- 命令的语法是：

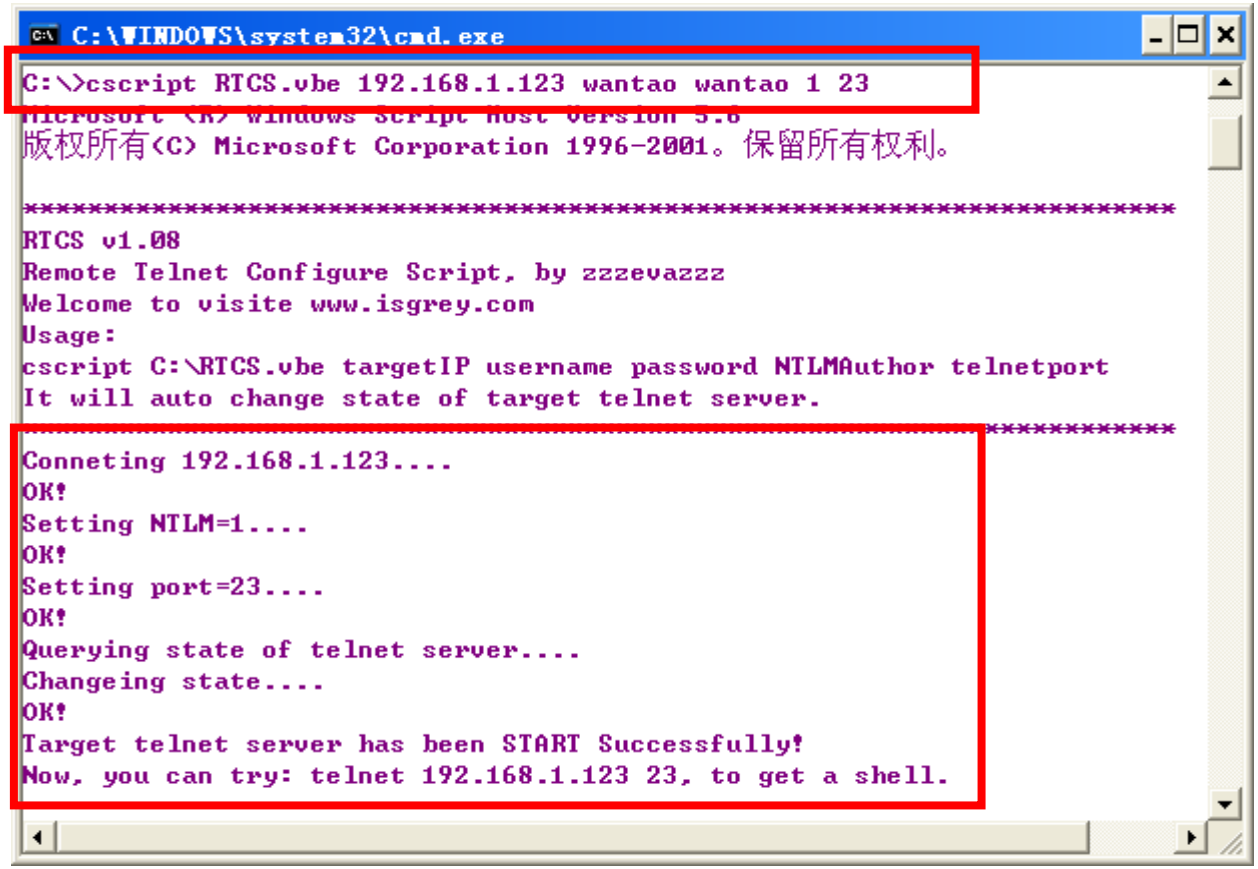
  “cscript RTCS.vbe 对方IP 用户名 密码 1 23”，其中cscript是操作系统自带的命令，RTCS.vbe是该工具软件脚本文件 ，1是登录系统的验证方式，23是Telnet开放的端口
- 该命令根据网络的速度，执行的时候需要一段时间



§8.7 网络后门与木马

➢ 一、远程启动Telnet服务——工具RTCS.vbe

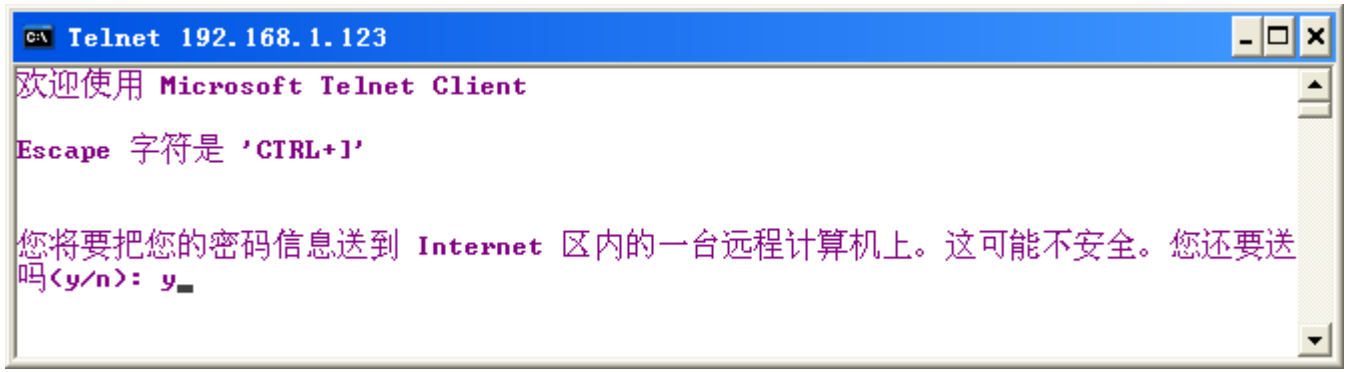
- 开启远程主机Telnet服务的过程



§8.7 网络后门与木马

一、远程启动Telnet服务——工具RTCS.vbe

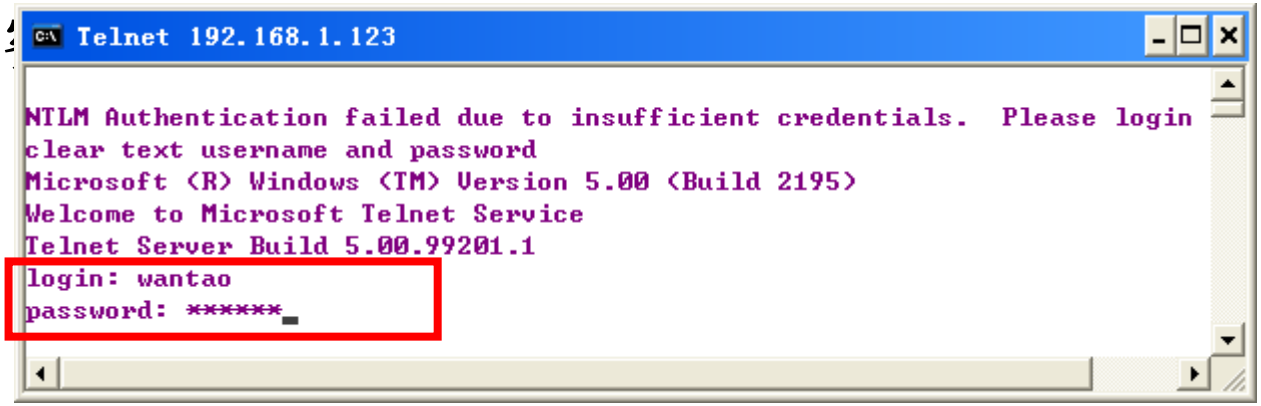
- 执行完成后，对方的Telnet服务就被开启了。在DOS提示符下，登录目标主机的Telnet服务
- 输入命令“Telnet 对方IP”，因为Telnet的用户名和密码是明文传递的，出现确认发送信息对话框



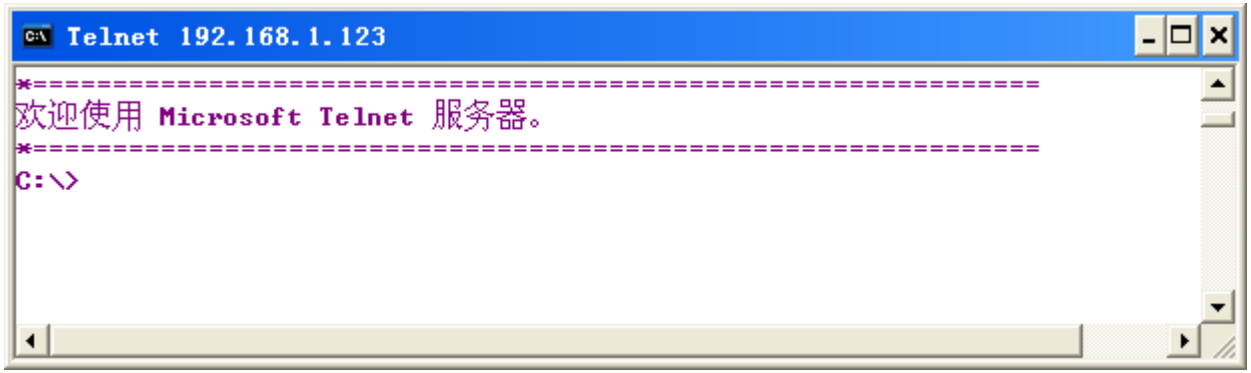
§8.7 网络后门与木马

➢ 一、远程启动Telnet服务——工具RTCS.vbe

- 输入字符“y”，进入Telnet的登录界面，需要输入主机的用户名和

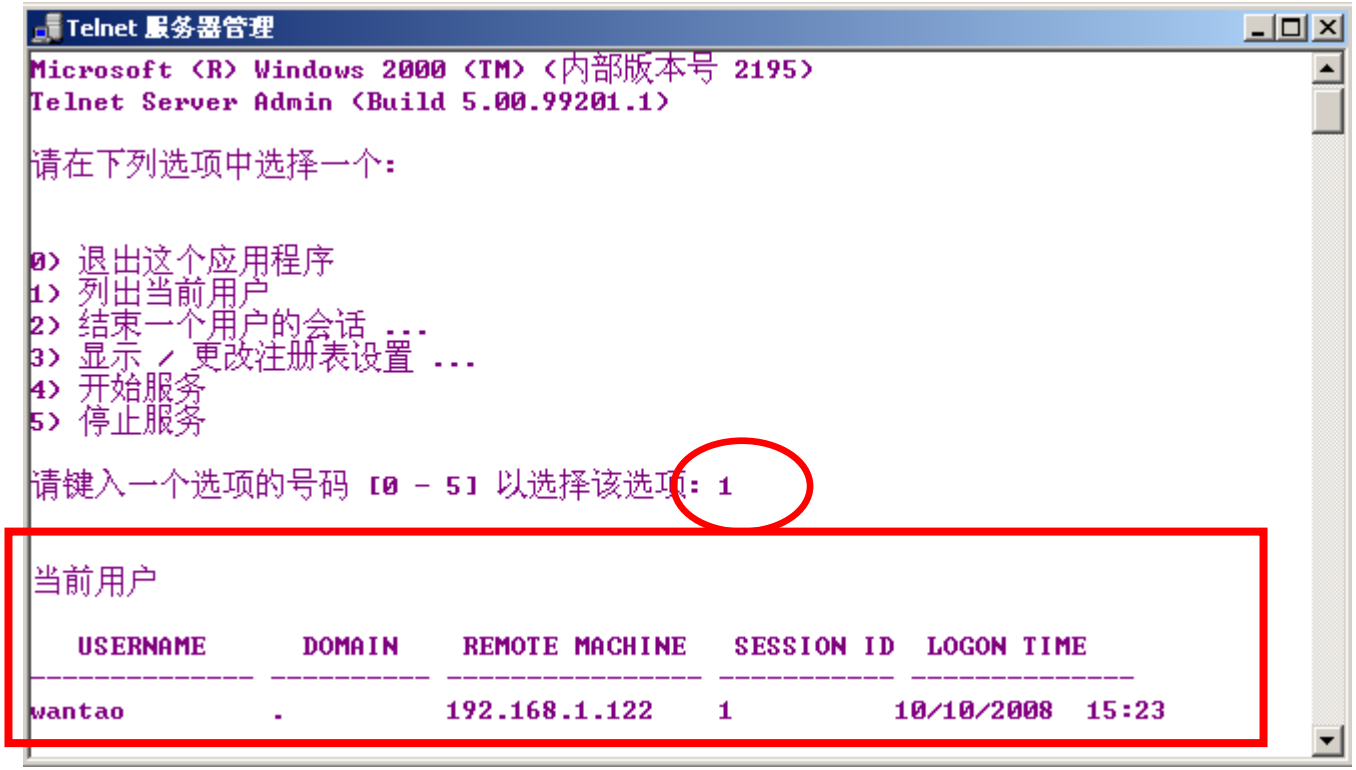


- 如果用户名和密码没有错误，将进入对方主机的命令行



§8.7 网络后门与木马

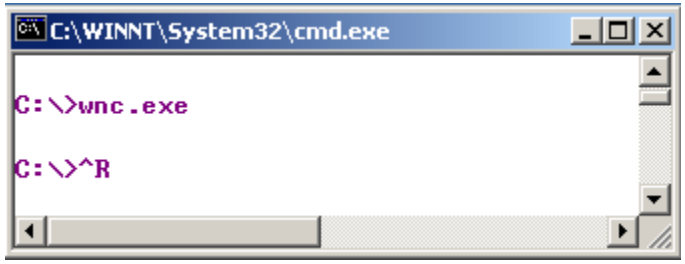
- 一、远程启动Telnet服务——工具RTCS.vbe



§8.7 网络后门与木马

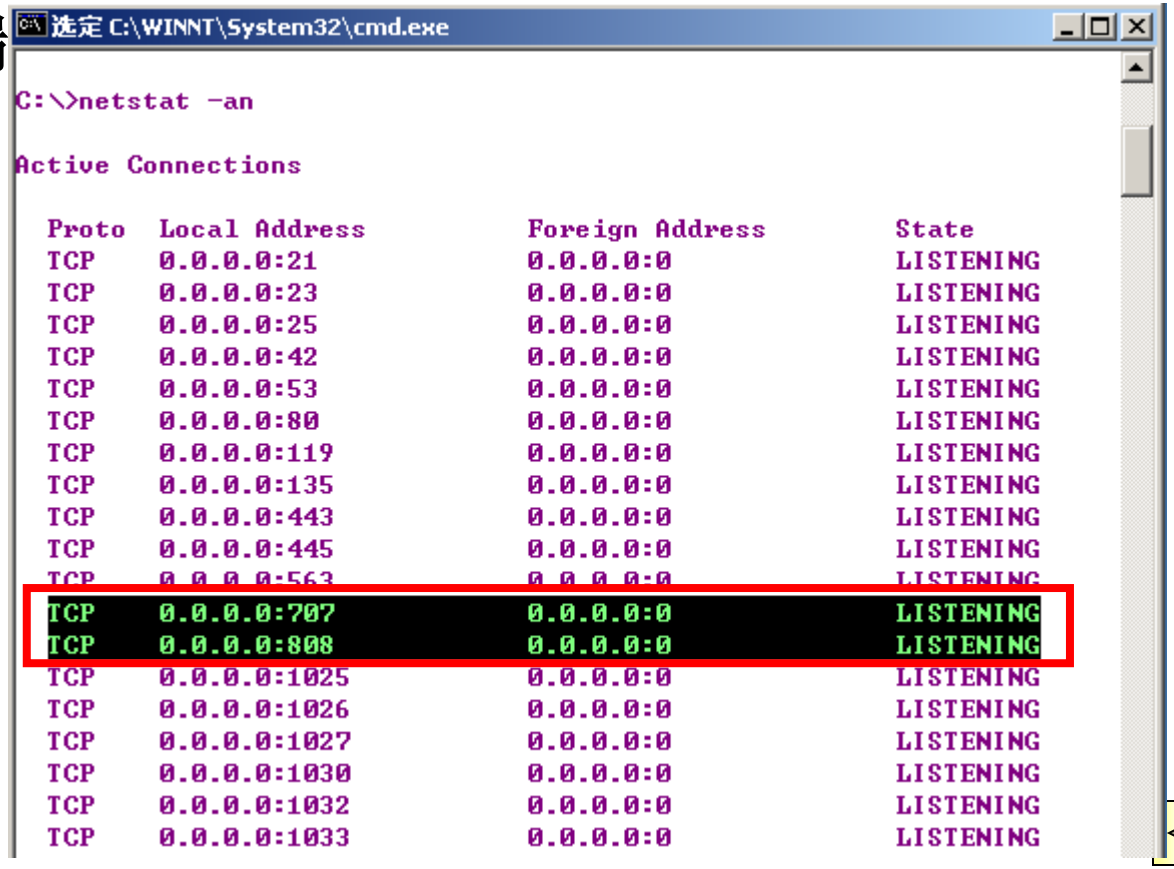
二、建立Web服务和Telnet服务——工具wnc.exe

- 工具软件wnc.exe可以在对方的主机上开启两个服务：Web服务和Telnet服务。其中Web服务的端口是808，Telnet服务的端口是707。只要在对方的命令行下执行wnc.exe就可以



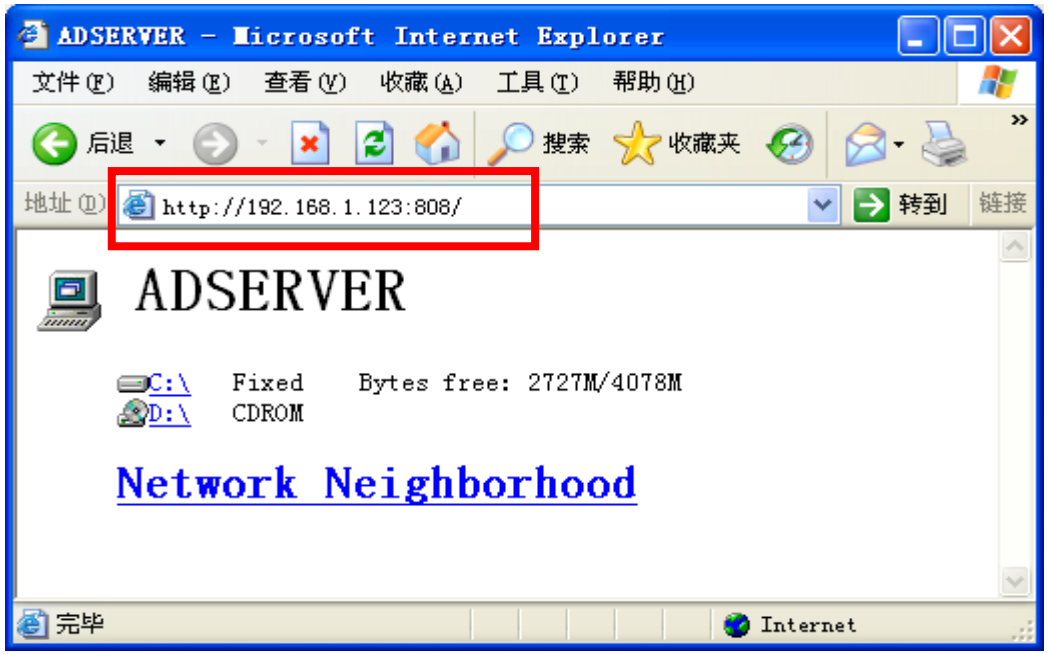
§8.7 网络后门与木马

- 二、建立Web服务和Telnet服务——工具wnc.exe
  - 执行完毕后，利用命令“netstat -an”来查看开启的808和707端



§8.7 网络后门与木马

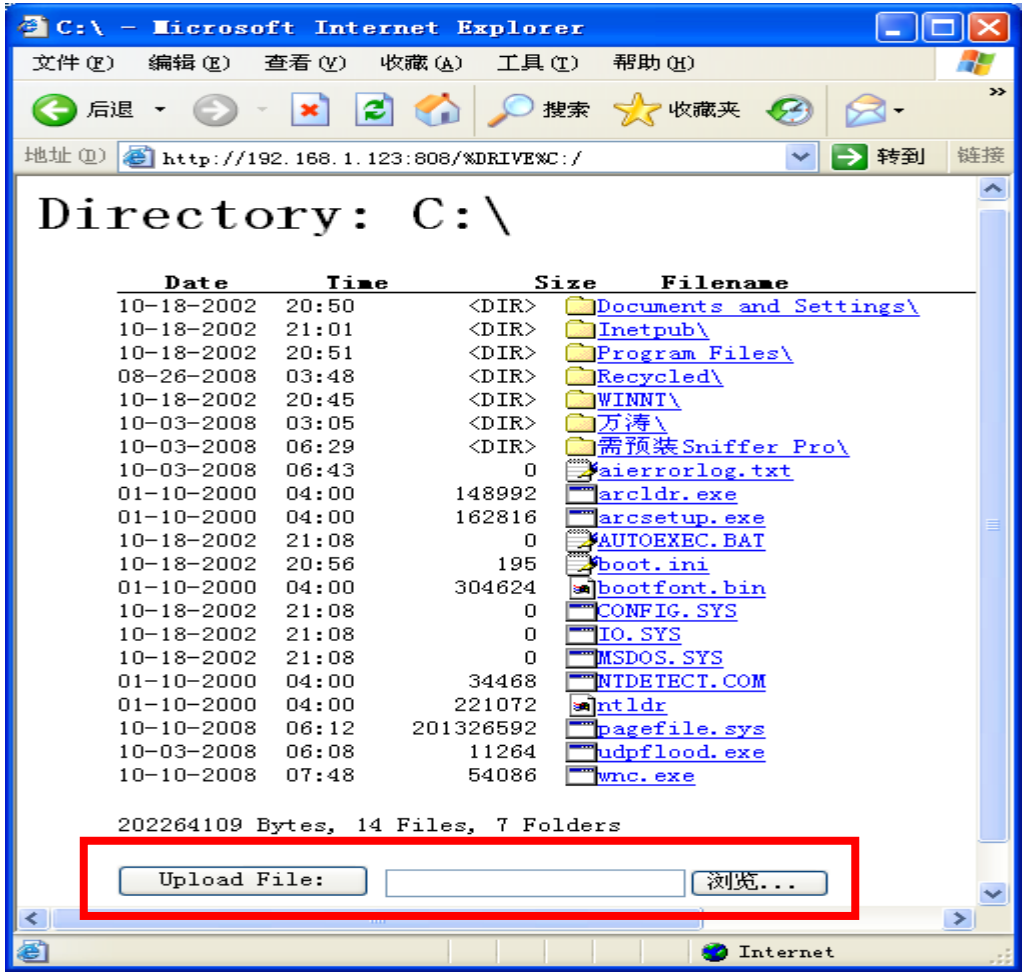
- 二、建立Web服务和Telnet服务——工具wnc.exe
  - 说明服务端口开启成功，可以连接该目标主机提供的这两个服务了。首先测试Web服务808端口，在浏览器地址栏中输入“http://对方IP:808”，出现主机的盘符列表



§8.7 网络后门与木马

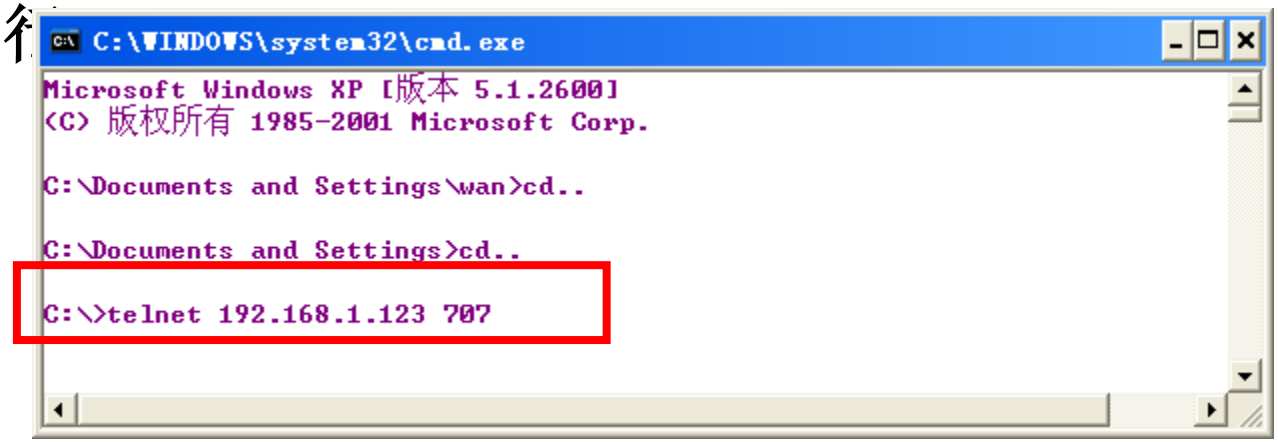
➢ 二、建立Web服务和Telnet服务——工具wnc.exe

- 可以向对方服务器下载和上传文件



§8.7 网络后门与木马

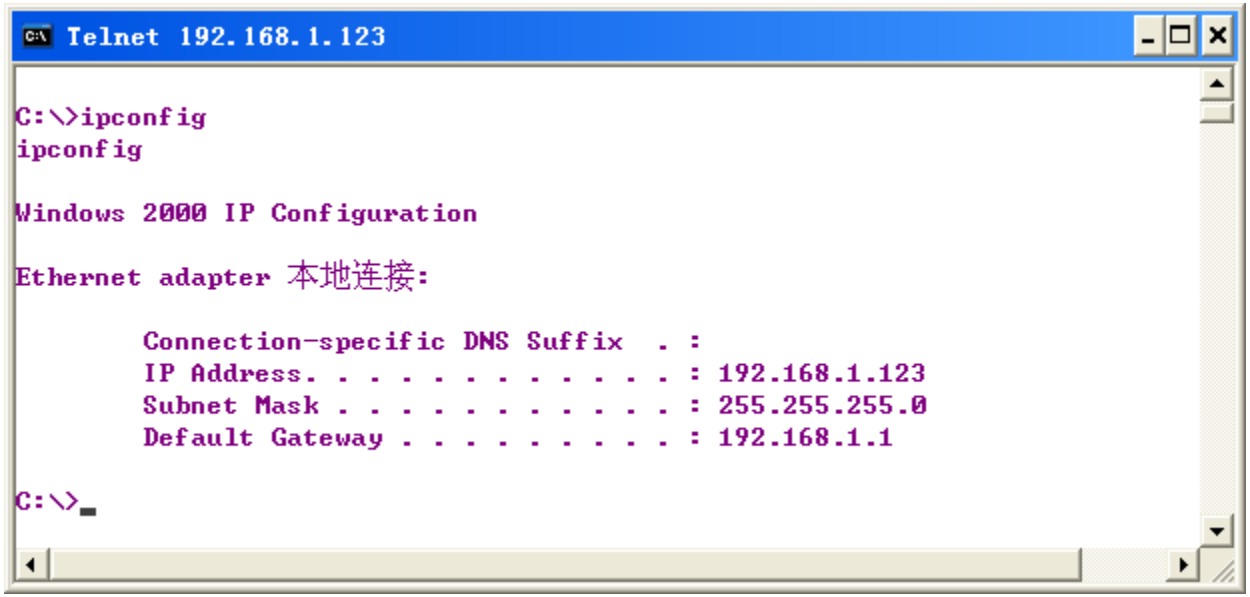
- 二、建立Web服务和Telnet服务——工具wnc.exe
  - 可以利用命令“telnet 对方IP 707” 登录到对方的命令行



§8.7 网络后门与木马

➢ 二、建立Web服务和Telnet服务——工具wnc.exe

- 不用任何的用户名和密码就登录了对方主机的命令行



§8.7 网络后门与木马

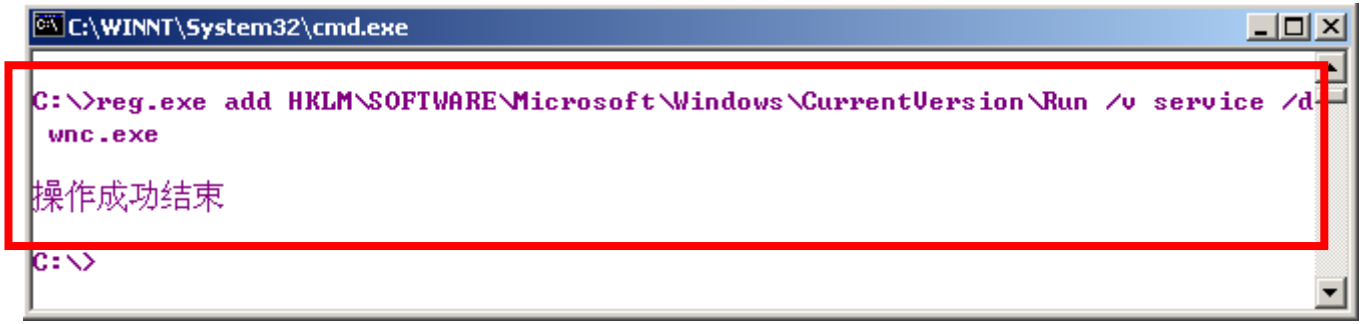
二、建立Web服务和Telnet服务——工具wnc.exe

- 通过707端口也可以方便的获得对方的管理员权限。
- wnc.exe的功能强大，但是该程序不能自动加载执行，需要将该文件加到自启动程序列表中。
- 一般将wnc.exe文件放到对方的winnt目录或者winnt/system32目录下，这两个目录是系统环境目录，执行这两个目录下的文件不需要给出具体的路径。

§8.7 网络后门与木马

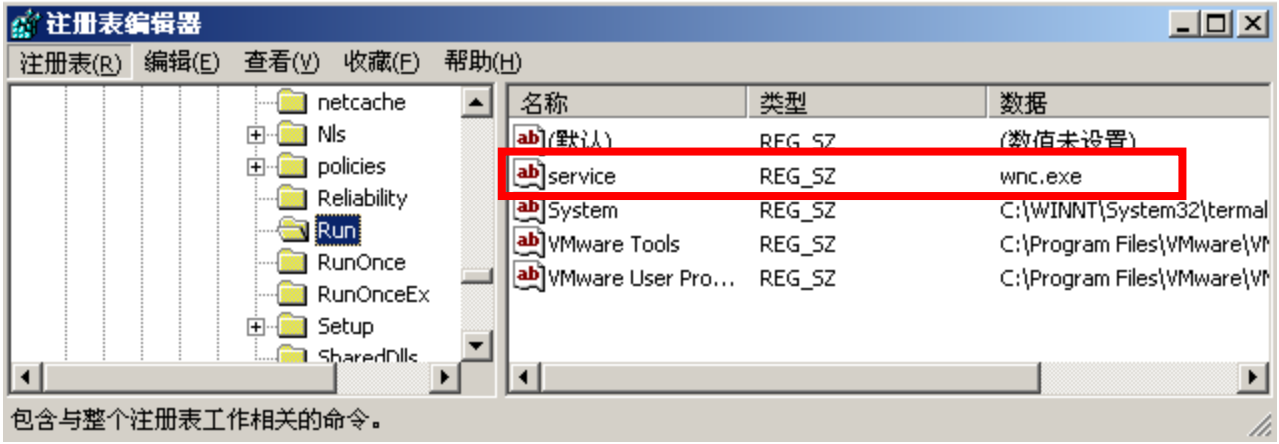
二、建立Web服务和Telnet服务——工具wnc.exe

- 将wnc.exe文件加入自启动程序列表的方法
  - 首先将wnc.exe和reg.exe文件拷贝对方的winnt目录下
  - 然后利用reg.exe文件将wnc.exe加载到注册表的自启动项目中，命令的格式为：“reg.exe add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v service /d wnc.exe”



§8.7 网络后门与木马

- 二、建立Web服务和Telnet服务——工具wnc.exe
  - 如果可以进入对方主机的图形界面，可以查看一下对方的注册表的自启动项，已经被修改



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

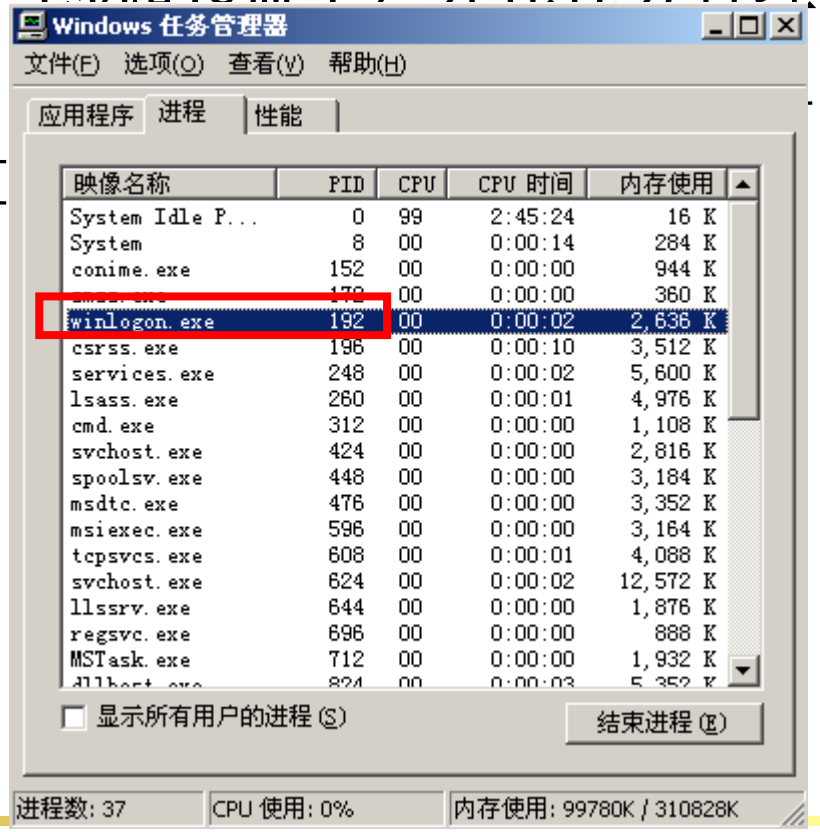
- 操作系统所有的用户信息都保存在注册表中
- 但是如果直接使用“regedit”命令打开注册表，该键值是隐藏的



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

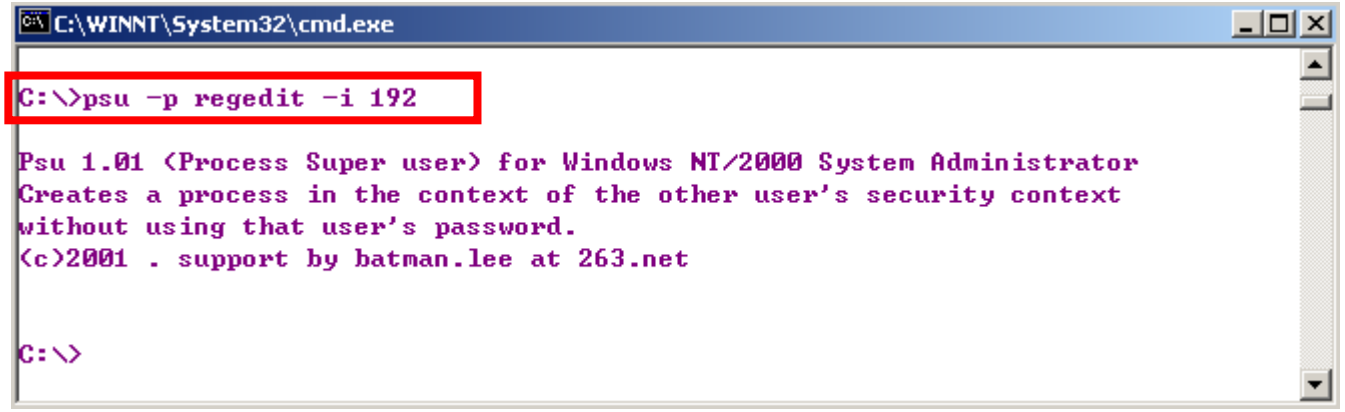
- 可以利用工具软件psu.exe得到该键值的查看和编辑权
- 将psu.exe拷贝对方主机的C盘下，并在任务管理器查看对方主机winlogon.exe文件查看该进程的I



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

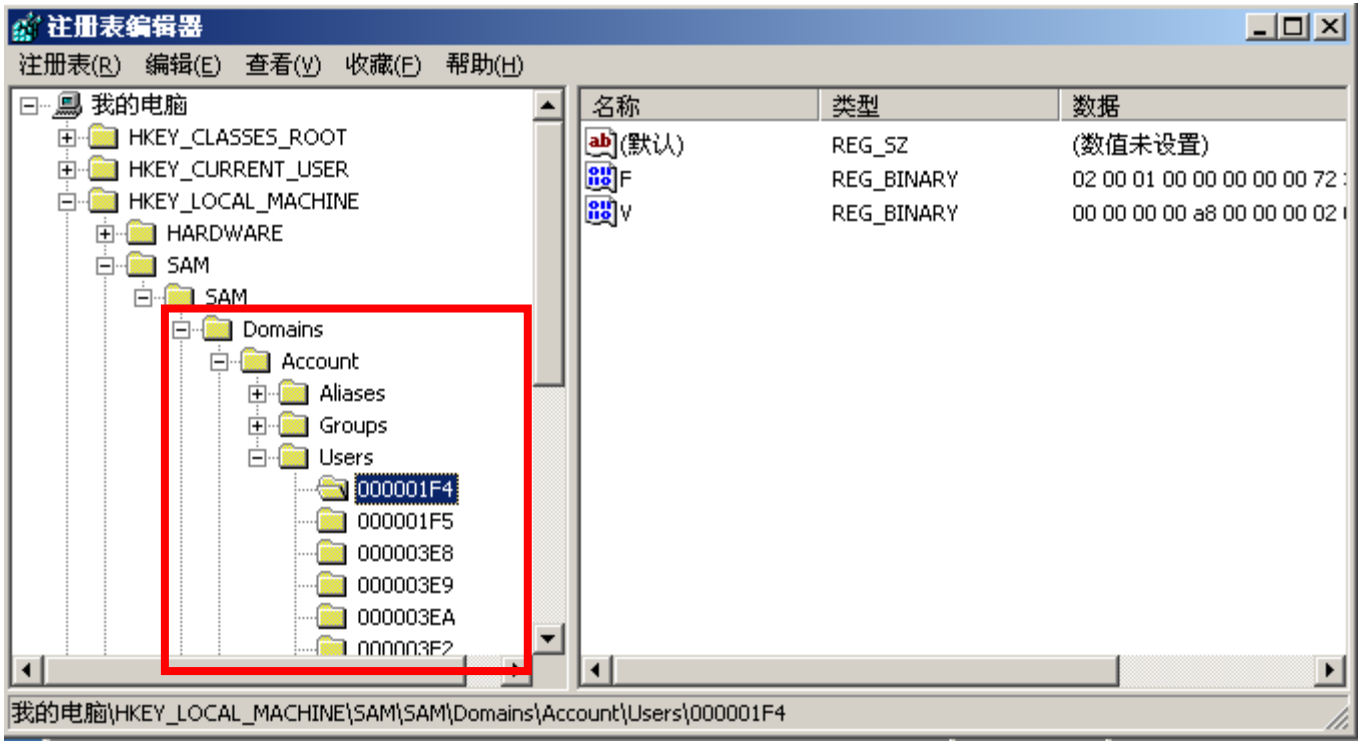
- 该进程号为192，下面执行命令“psu -p regedit -i pid”其中pid为Winlogon.exe的进程号



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

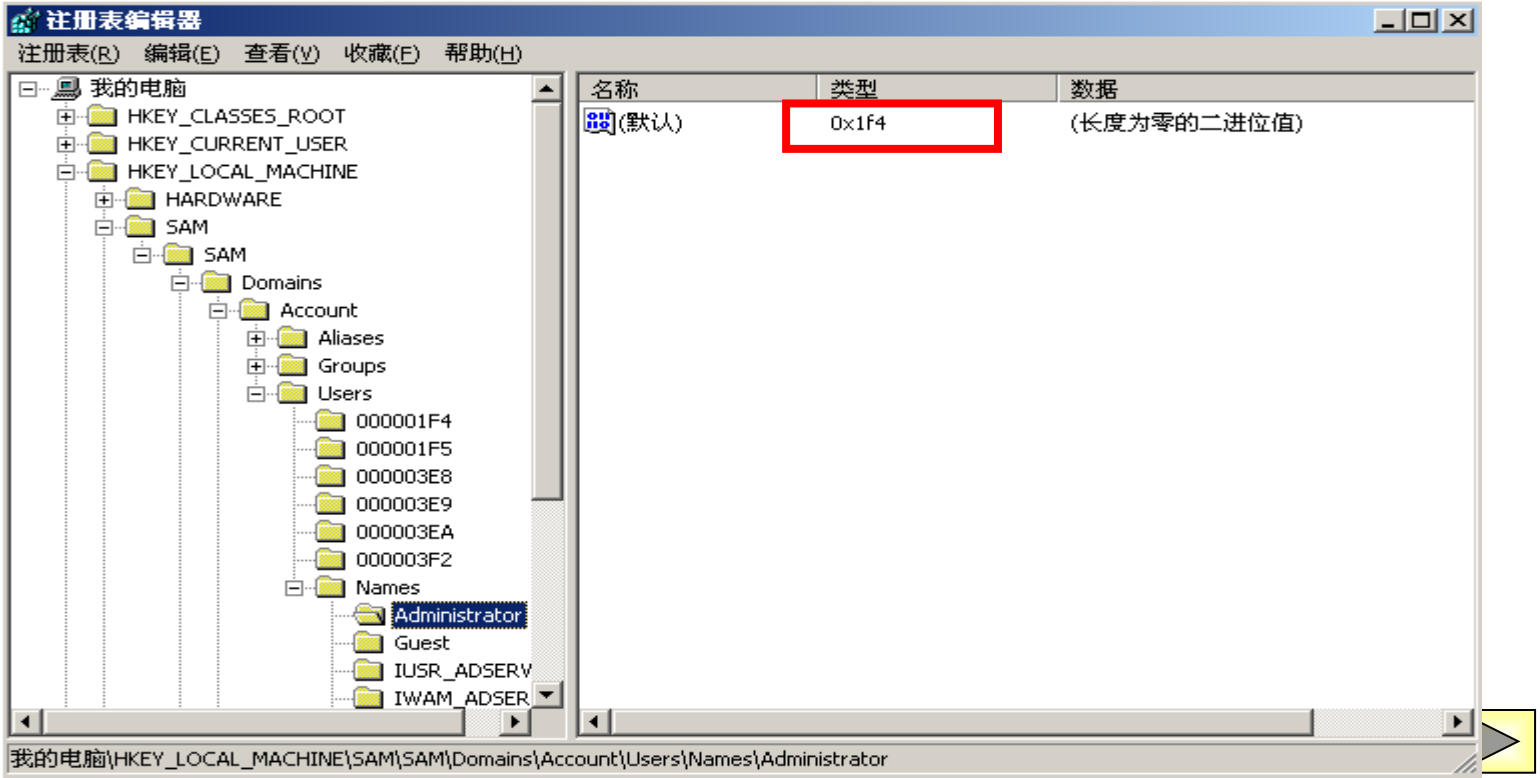
- 在执行该命令的时候必须将注册表关闭，执行完命令以后，注册表编辑器被自动打开，查看SAM下的键值



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

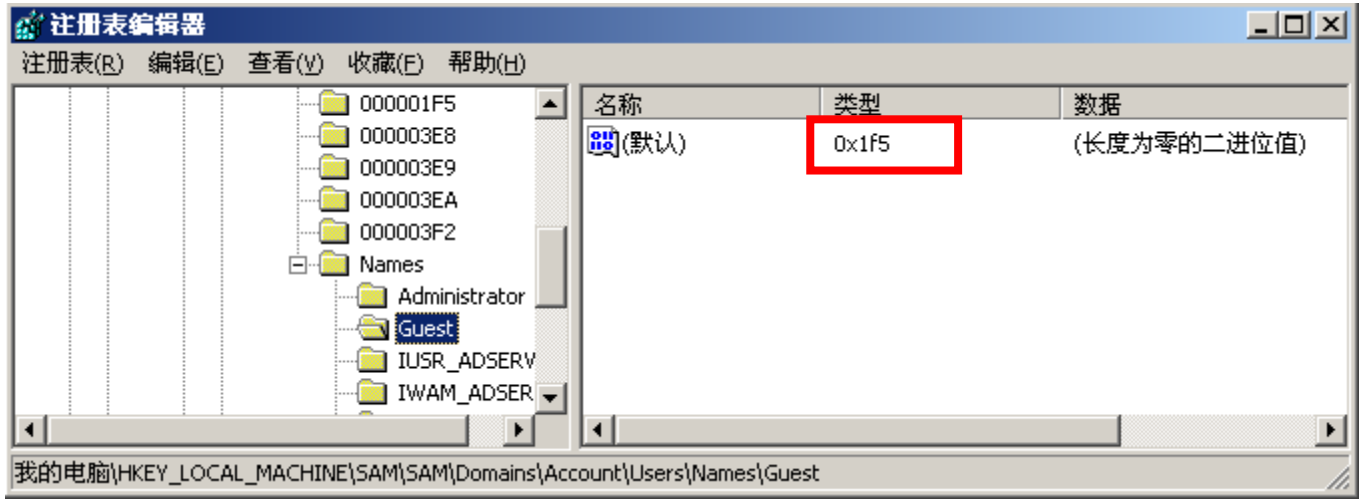
- 查看Administrator和guest默认的键值
- Windows 2000操作系统上，Administrator一般为0x1f4，



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

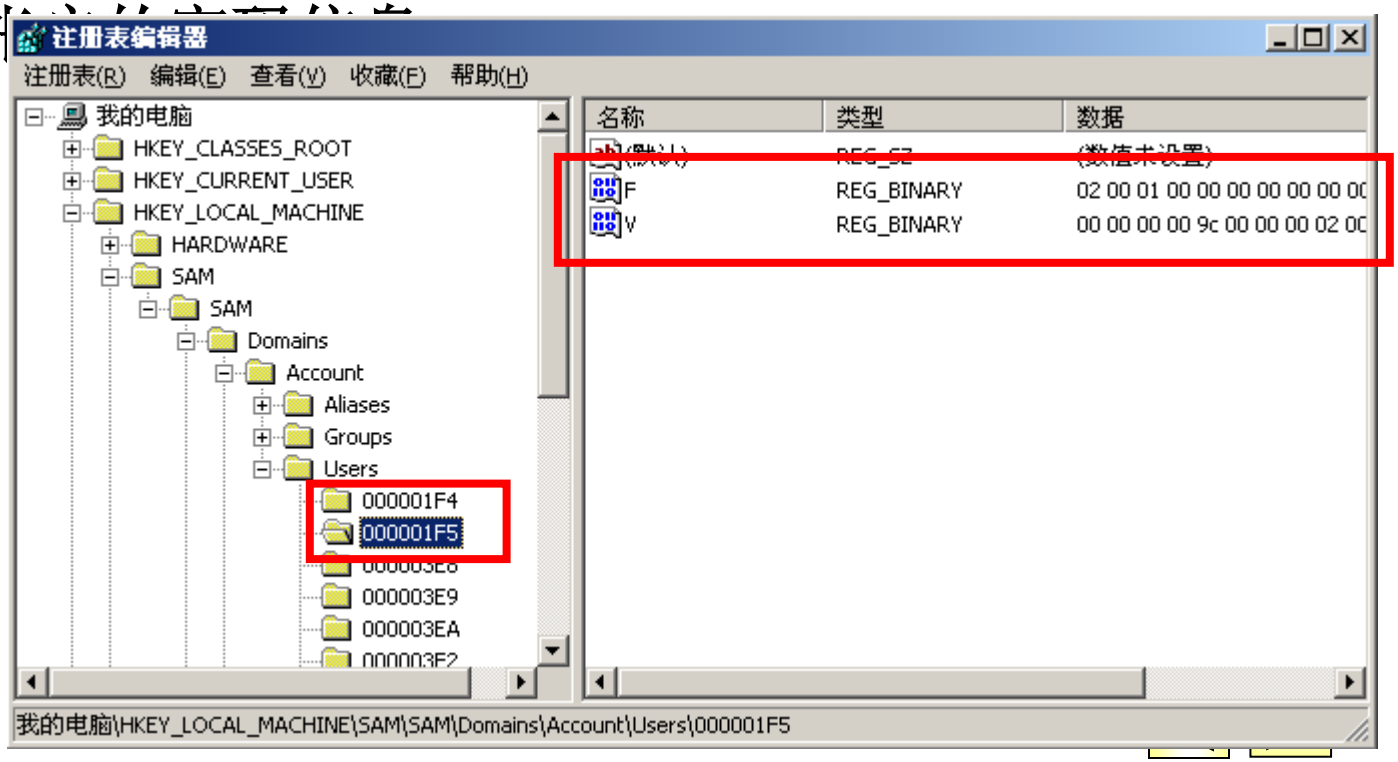
- 查看Administrator和guest默认的键值
- Windows 2000操作系统上，Administrator一般为0x1f4，guest一般为0x1f5



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

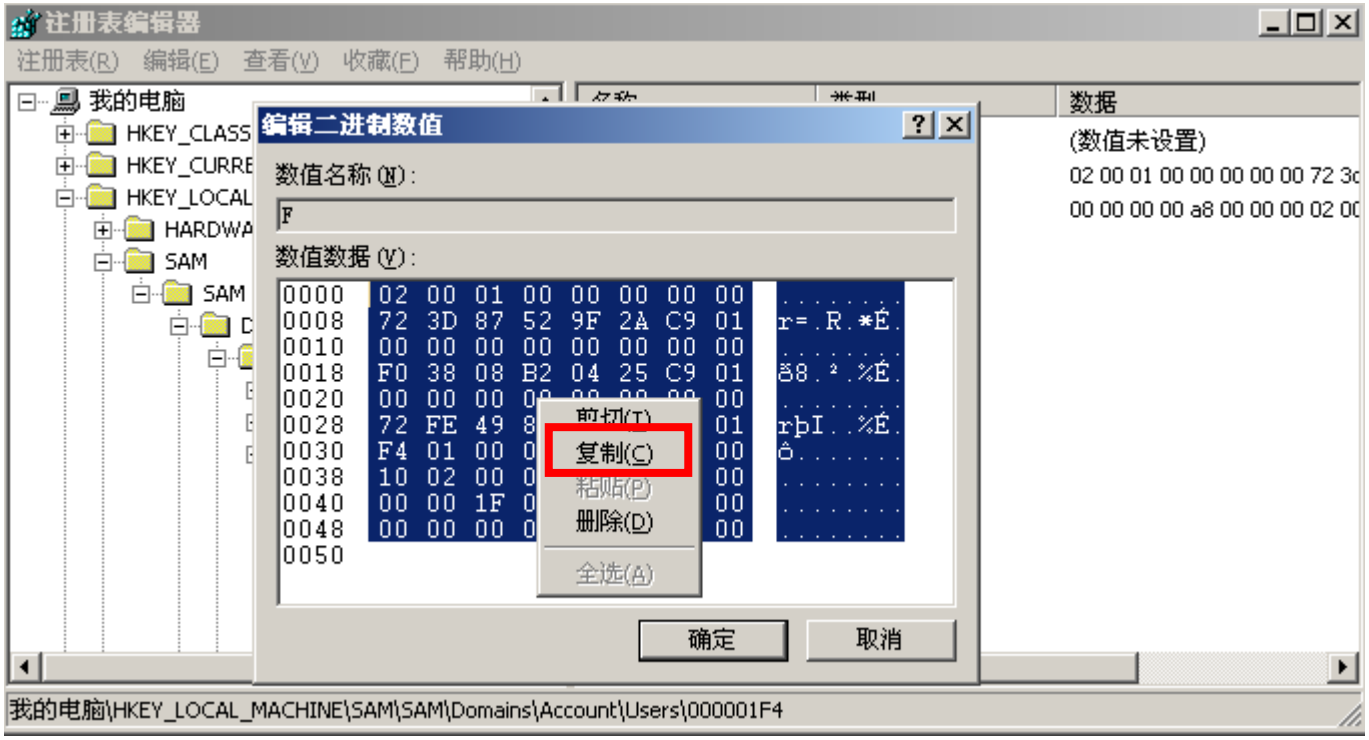
- 帐户配置信息：根据“0x1f4”和“0x1f5”找到Administrator和guest帐户的配置信息，右栏目F键值中保存了帐



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

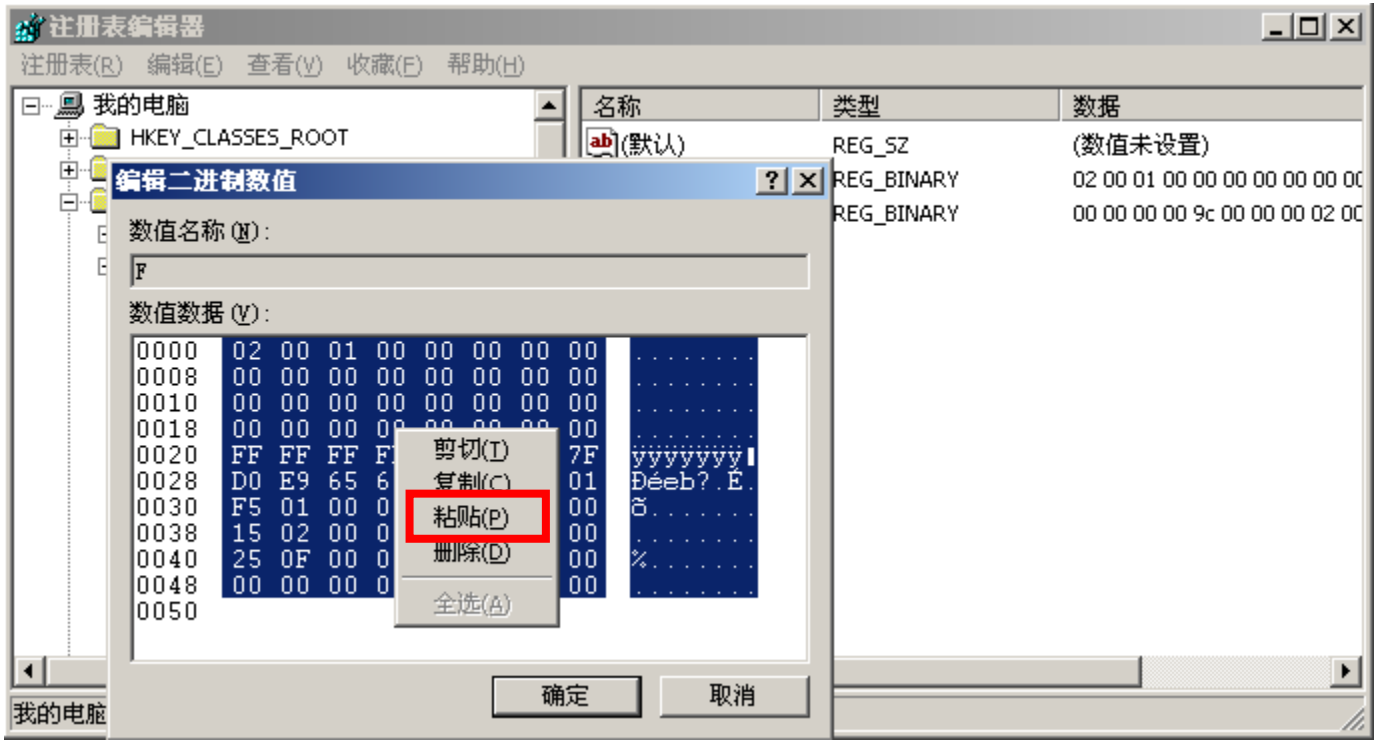
- 拷贝管理员配置信息：双击“000001F4”目录下键值“F”，将看到的这些二进制信息全选，并拷贝到出来。



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

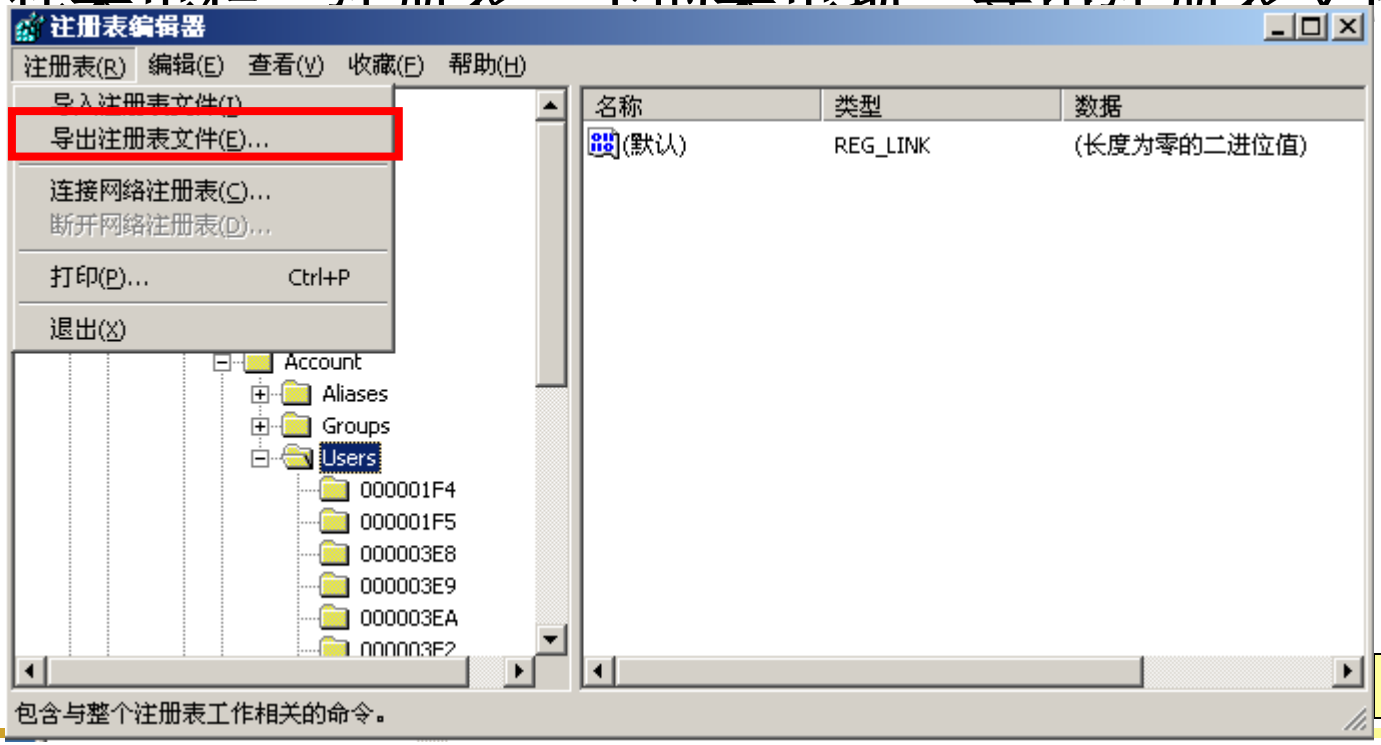
- 覆盖Guest用户的配置信息：将拷贝出来的信息全部覆盖到“000001F5”目录下的“F”键值中， Guest帐户就具



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

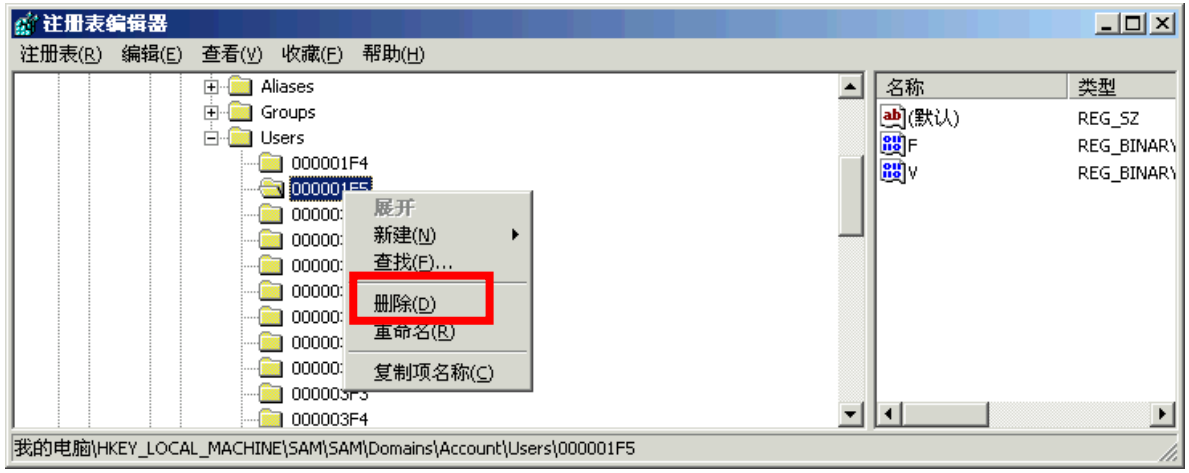
- 保存键值：为了能够使Guest帐户在禁用的状态登录，需要将Guest帐户信息导出注册表。选择User目录，然后选择菜单栏“注册表”下的菜单项“导出注册表文件”，将



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

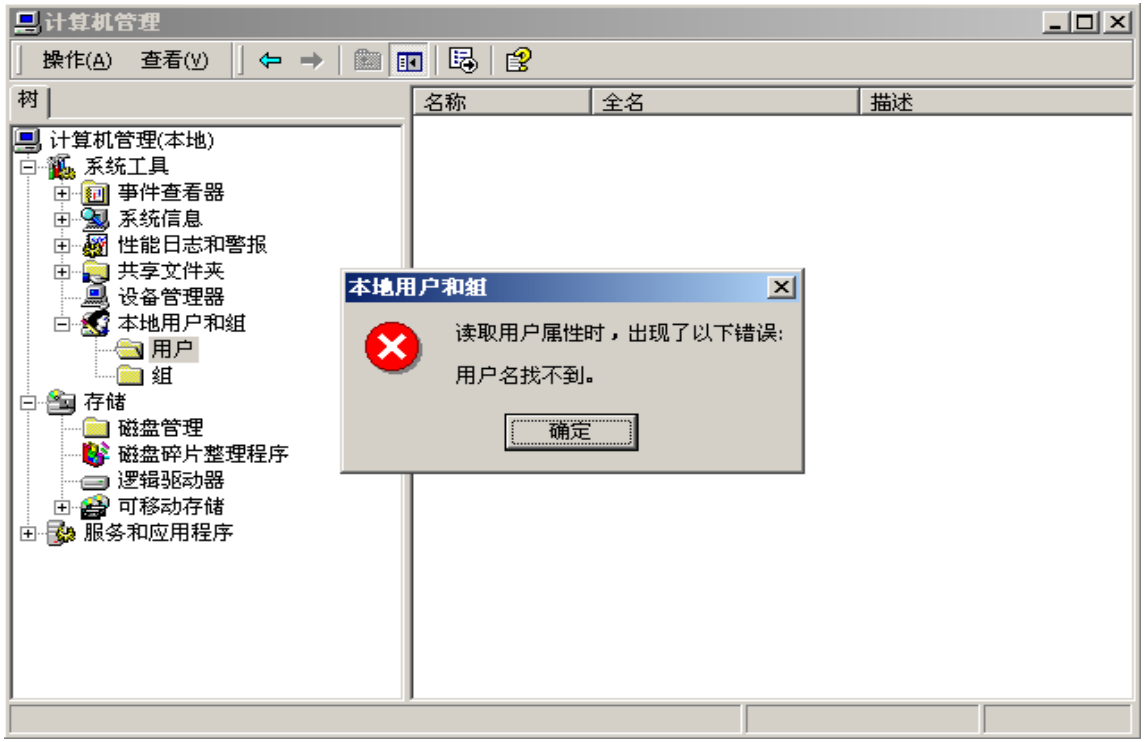
- 删除Guest帐户信息：打开计算机管理对话框，并在注册表中分别删除Guest和“00001F5”两个目录



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

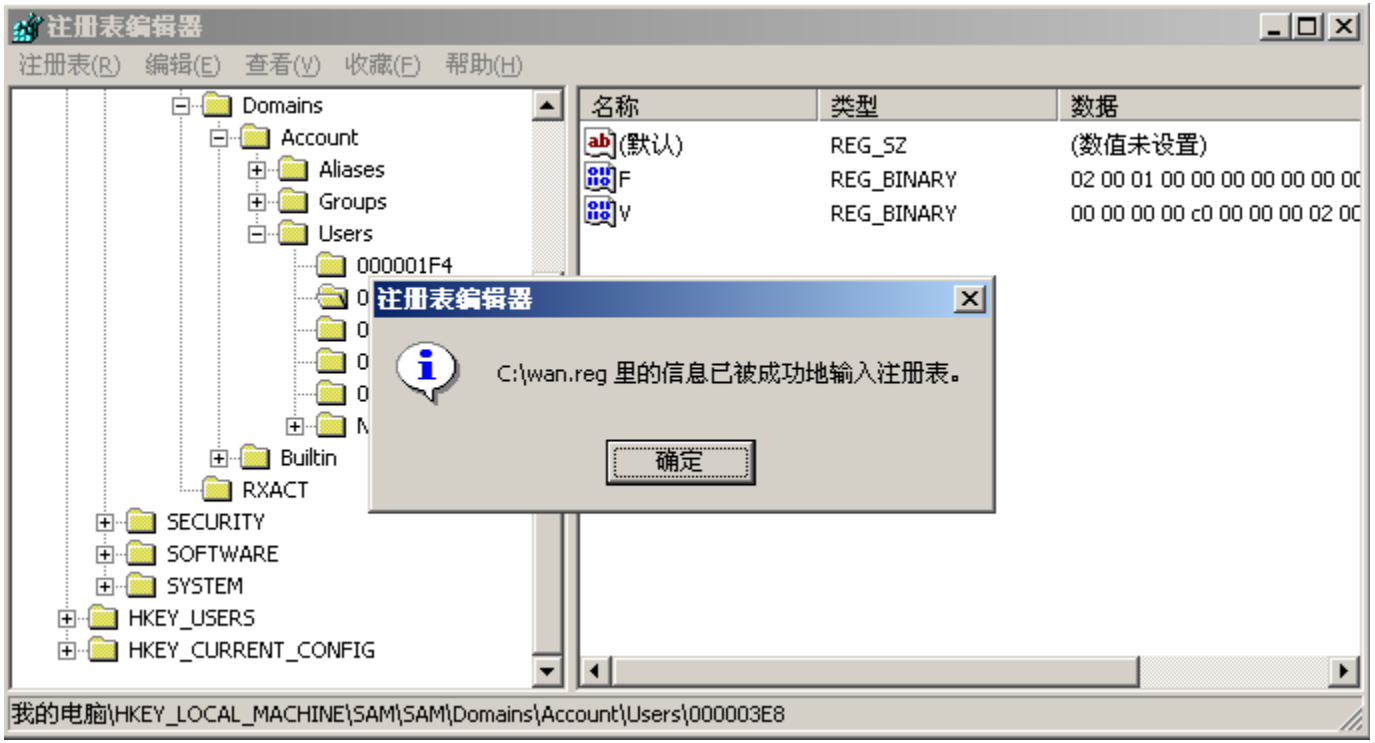
- 刷新用户列表 ：这个刷新对方主机的用户列表，会出现用户找不到的对话框



§8.7 网络后门与木马

➢ 三、让禁用的Guest具有管理员权限

- 将刚才导出的信息文件导入注册表

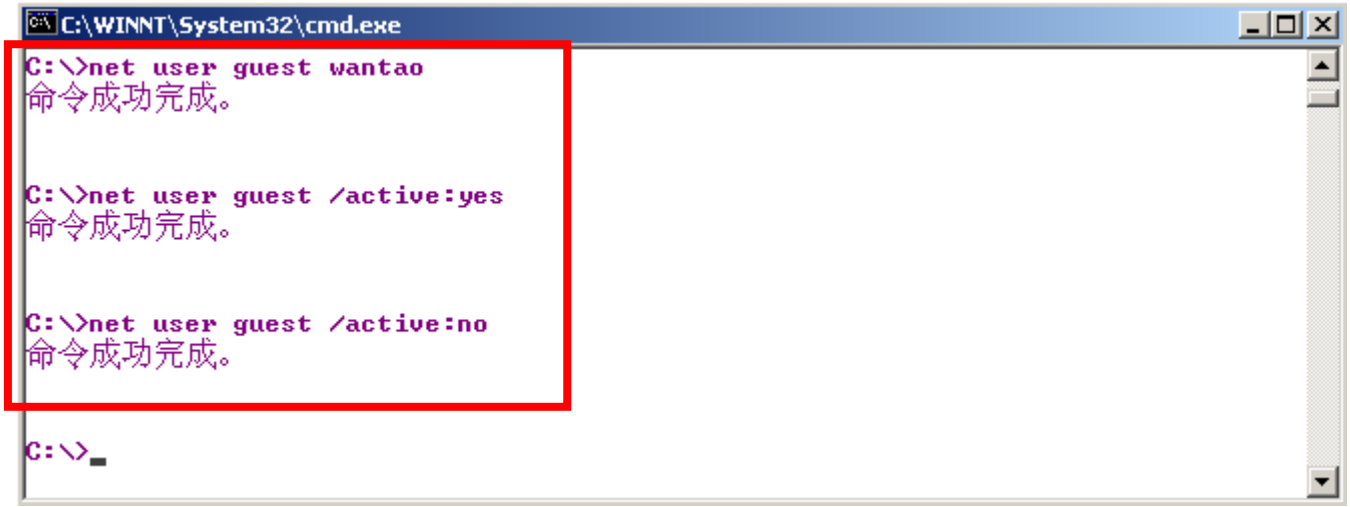


- 然后刷新用户列表就不会出现刚才的对话框了

§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

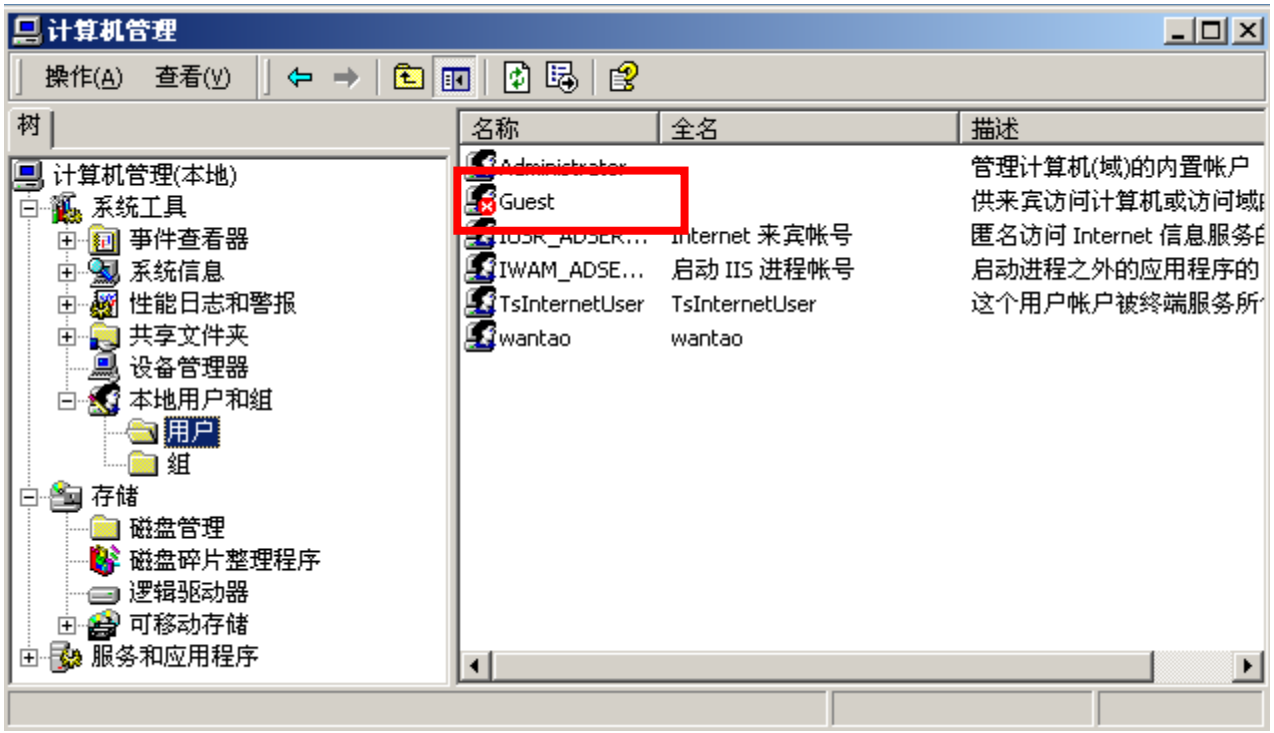
- 接着在对方主机的命令行下修改Guest的用户属性
- 首先修改Guest帐户的密码，比如改成“wantao”，并将Guest帐户开启和停止



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

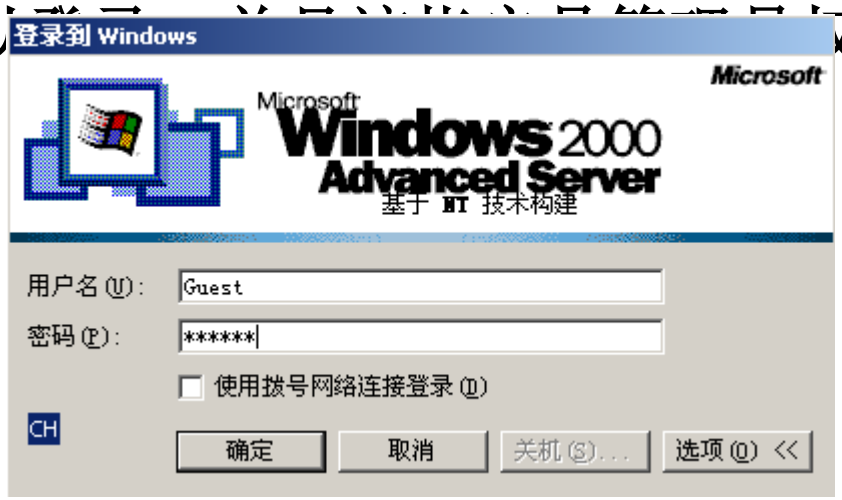
- 查看guest帐户属性：再查看一下计算机管理窗口中的Guest帐户，发现该帐户是禁用的



§8.7 网络后门与木马

三、让禁用的Guest具有管理员权限

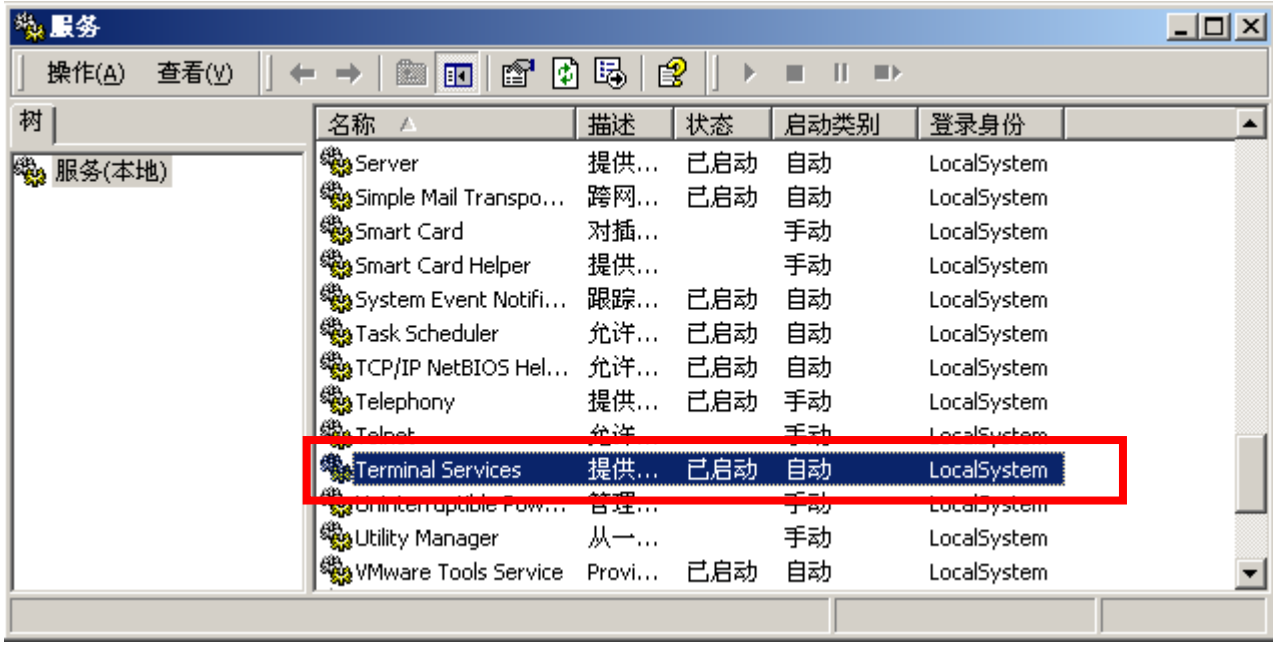
- 利用禁用的guest帐户登录
  - 注销退出系统
  - 然后用用户名：“guest”，密码：“wantao”登录系统
  - 可以[illegible]权限



§8.7 网络后门与木马

四、连接终端服务的软件

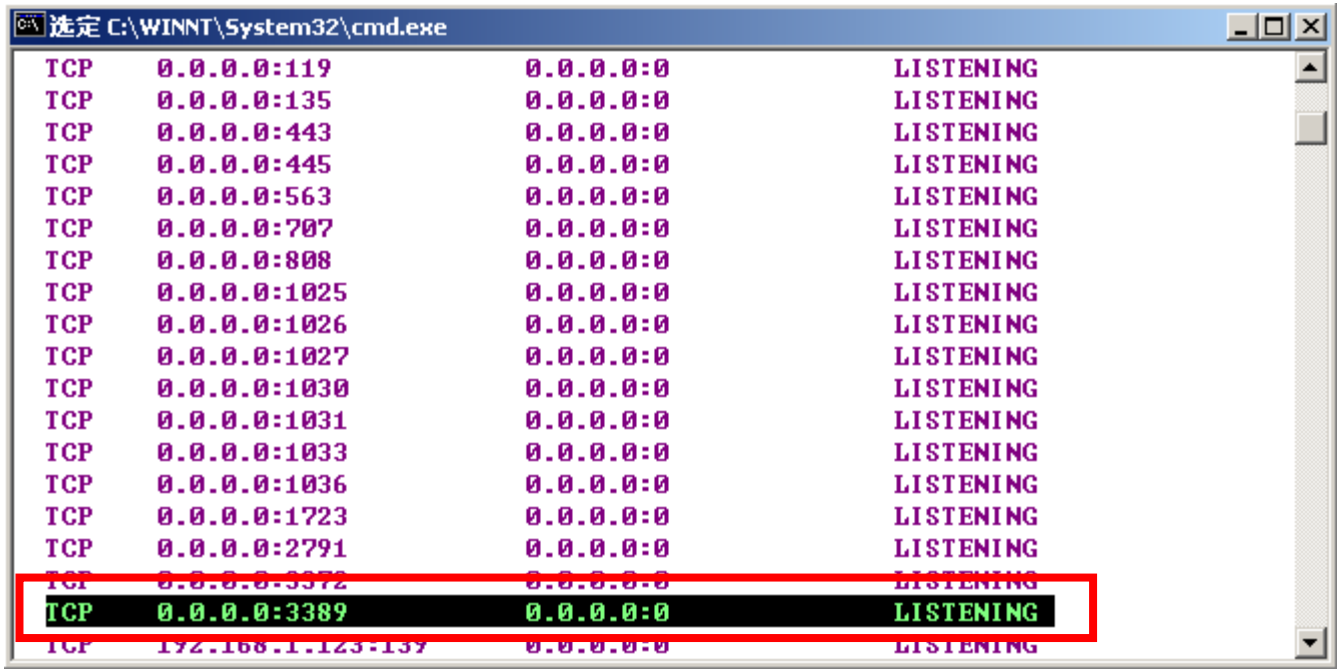
- 终端服务是Windows操作系统自带的，可以远程通过图形界面操纵服务器。在默认的情况下终端服务的端口号是3389。可以在系统服务中查看终端服务是否启动



§8.7 网络后门与木马

四、连接终端服务的软件

- 服务默认的端口是3389，可以利用命令“netstat -an”来查看该端口是否开放



§8.7 网络后门与木马

四、连接终端服务的软件

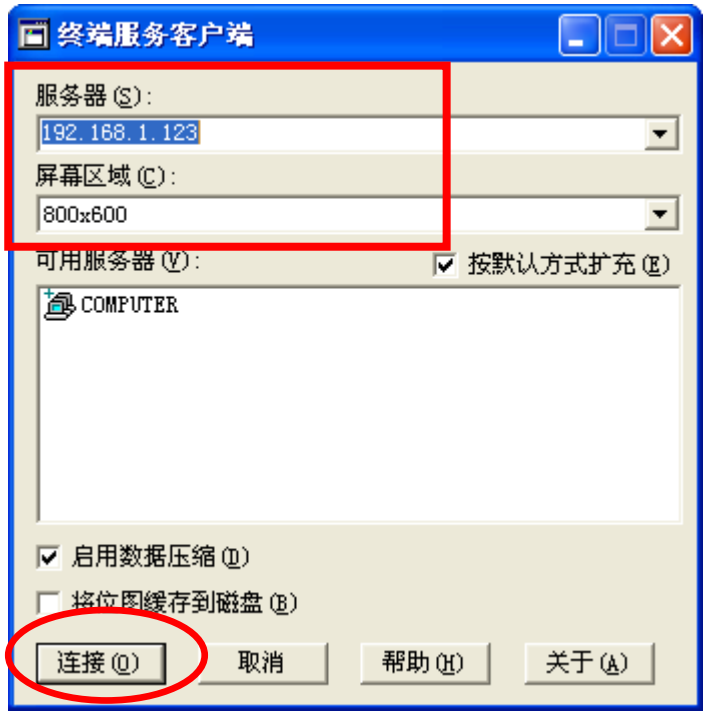
- 管理员为了远程操作方便，服务器上的该服务一般都是开启的。这就给黑客们提供一条可以远程图形化操作主机的途径。
- 利用该服务，目前常用的有三种方法连接到对方主机
  - 使用Windows 2000的远程桌面连接工具
  - 使用Windows XP的远程桌面连接工具
  - 使用基于浏览器方式的连接工具

§8.7 网络后门与木马

➢ 四、连接终端服务的软件

——Windows 2000自带的终端服务工具mstsc.exe

- 该工具只要设置要连接主机的IP地址和连接桌面的分辨率就可以



§8.7 网络后门与木马

➢ 四、连接终端服务的软件

——Windows 2000自带的终端服务工具mstsc.exe

- 如果目标主机的终端服务是启动的，可以直接登录到对方的桌面，在登录框输入用户名和密码就可以在图形化界面种操纵对方主



§8.7 网络后门与木马

- 四、连接终端服务的软件

Windows 2000自带的终端服务工具mstsc.exe

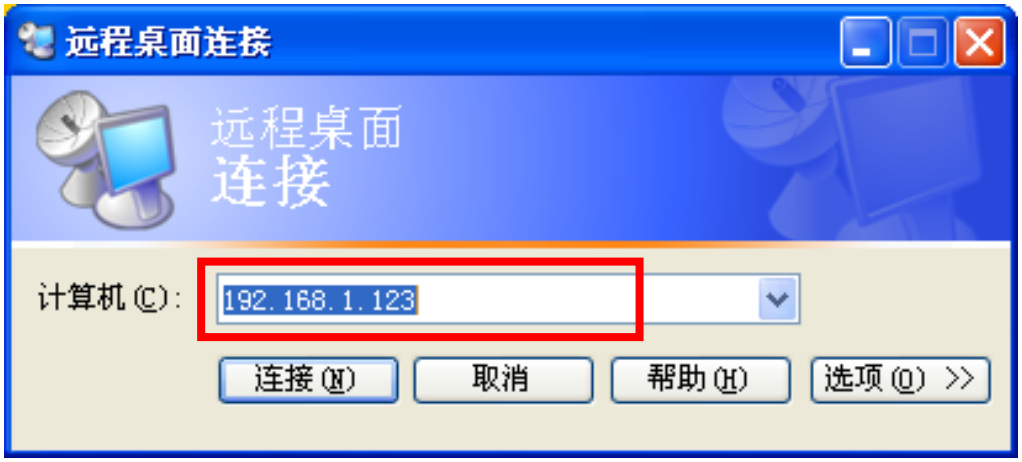


§8.7 网络后门与木马

➢ 四、连接终端服务的软件

——Windows XP自带的终端服务工具mstsc.exe

- 界面简单，只要输入对方的IP地址就可以了

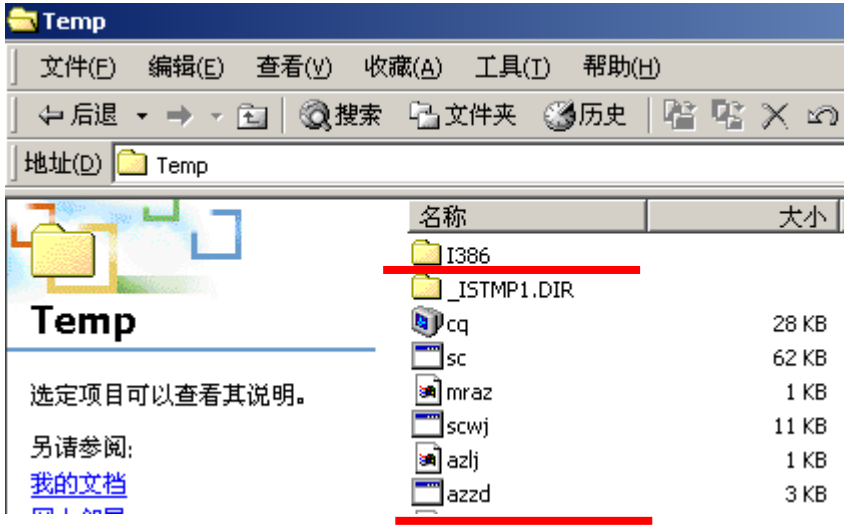


§8.7 网络后门与木马

- 五、安装并启动终端服务——工具软件djxyxs.exe
  - 假设对方不仅没有开启终端服务，而且没有安装终端服务所需要的软件。
  - 工具软件djxyxs.exe可以给对方安装并开启该服务。在该工具软件中已经包含了安装终端服务所需要的所有文件

§8.7 网络后门与木马

- 五、安装并启动终端服务——工具软件djxyxs.exe
  - 将该文件上传并拷贝到对方服务器的Winnt\temp目录下
  - 然后执行djxyxs.exe文件，该文件会自动进行解压将文件全部放置到当前的目录下



§8.7 网络后门与木马

- 木马是一种可以驻留在对方系统中的一种程序。
- 木马一般由两部分组成：服务器端和客户端。
- 服务器端程序安装在被控制计算机中，一般通过电子邮件等手段让用户在其计算机中运行，达到控制该计算机的目的。
- 客户端程序是控制者所使用的，用于对受控的计算机进行控制。服务器端程序和客户端程序建立起连接就可以实现对远程计算机的控制了。
- 木马运行时，首先服务器端获得本地计算机的最高操作权限，当本地计算机连入网络后，客户端可与服务器端建立连接，并向服务器端发送各种基本的操作请求，由服务器端完成这些请求，即实现对本地计算机的控制了。

§8.7 网络后门与木马

- 木马本身不具备繁殖性和自动感染的功能。
- 木马程序表面上看上去没有任何的损害，实际隐藏着可以控制用户整个计算机系统、打开后门等危害系统安全的功能
- Windows下的木马有：Netbus、subseven、BO、冰河、网络神偷等。Unix下的木马有：Rhost ++、Login后门、rootkit等

§8.7 网络后门与木马

- 木马分类：
  - 远程访问型木马
  - 密码发送型木马
  - 键盘记录型木马
  - 毁坏型木马
  - FTP 型木马

- 最广泛使用的特洛伊木马
- 木马的目的是找到所有的隐藏密码，
- 木马简单，唯一做的事情就是记录
- 唯一功能是毁坏并删除文件
- 打开用户计算机的21端口
- 使每一个人都可以用一个FTP 客户端程序而不用密码连接到该计算机，并且可以进行最高权限的上传下载。

的冰河等。

§8.7 网络后门与木马

- 木马常用欺骗法：
  - 捆绑欺骗：如把木马服务端和某个游戏捆绑成一个文件在邮件中发给别人
  - 危险下载点：攻破一些下载站点后，下载几个下载量大的软件，捆绑上木马，再悄悄放回去让别人下载 ；或直接将木马改名上载到FTP 网站上，等待别人下载
  - 文件夹惯性点击：把木马文件伪装成文件夹图标后，放在一个文件夹中，然后在外面再套三四个空文件夹
  - zip 伪装：将一个木马和一个损坏的 zip 包捆绑在一起，然后指定捆绑后的文件为 zip 图标

§8.7 网络后门与木马

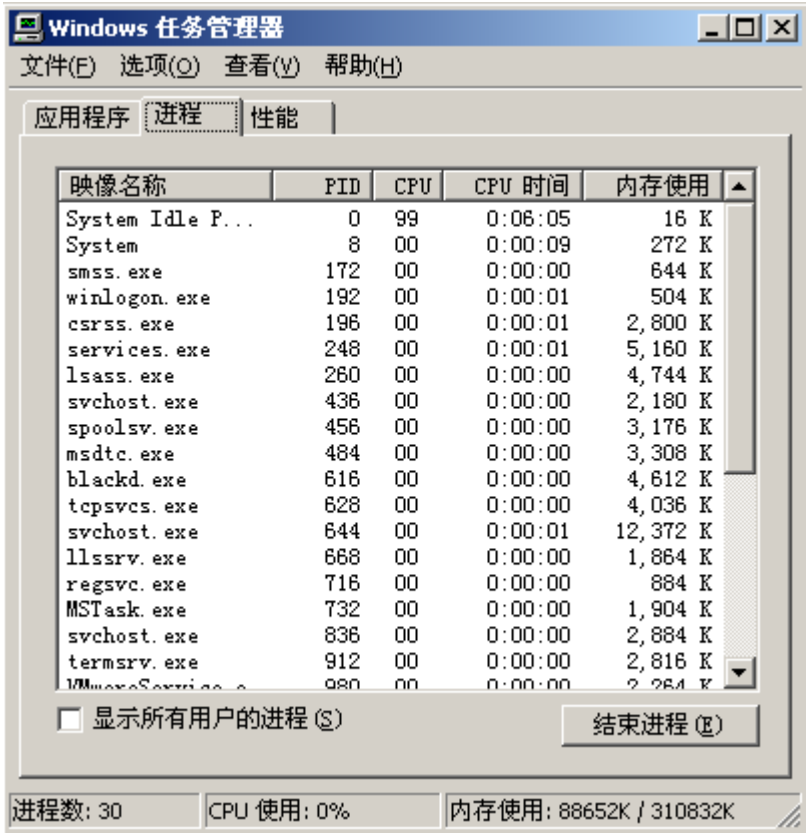
- 针对木马攻击的防范措施
  - 安装防火墙，禁止访问不该访问的服务端口，使用NAT隐藏内部网络结构
  - 安装防病毒软件
  - 提高安全意识，尽量避免使用来历不明的软件

§8.8 物理攻击与防范

- 物理安全是保护一些比较重要的设备不被接触。
- 物理安全比较难防，因为攻击往往来自能够接触到物理设备的用户。

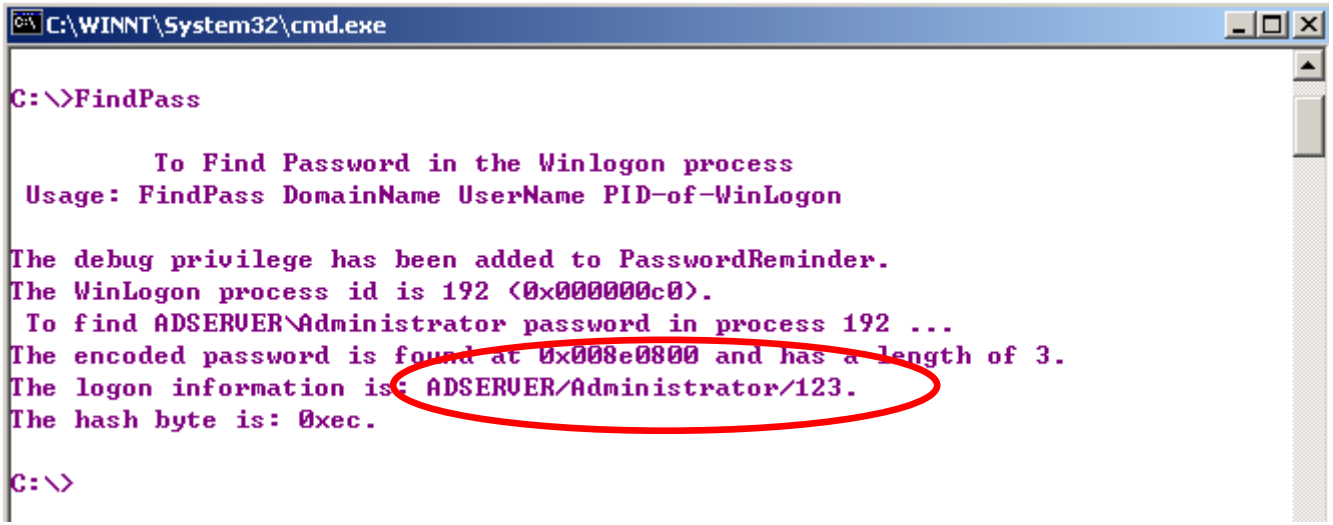
§8.8 物理攻击与防范

- 获取管理员密码——工具软件FindPass.exe
  - 登录后用户所有信息都存储在系统的进程winlogon.exe中



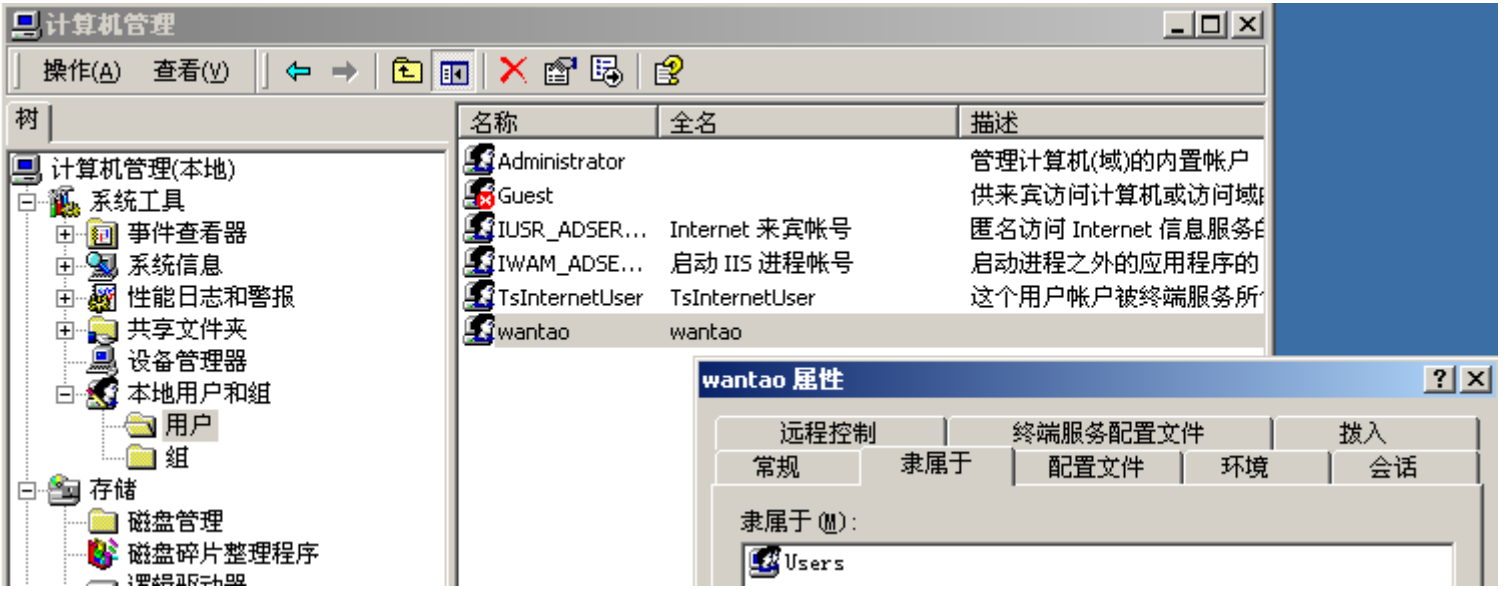
§8.8 物理攻击与防范

- 获取管理员密码——工具软件FindPass.exe
  - 将FindPass.exe拷贝到C根目录下，使用命令行执行



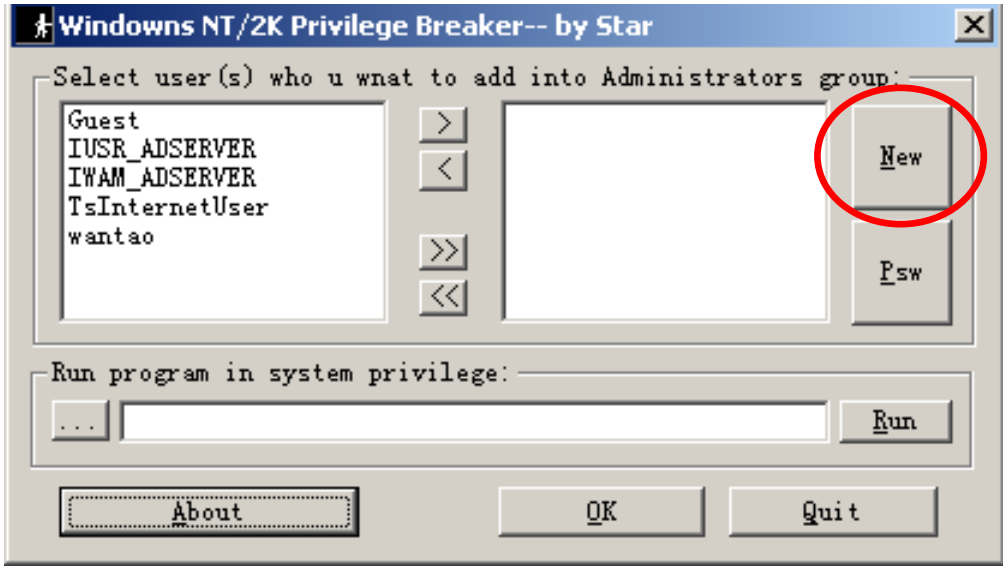
§8.8 物理攻击与防范

- 提升管理员权限——工具软件GetAdmin.exe
  - 使用Users类型用户登陆



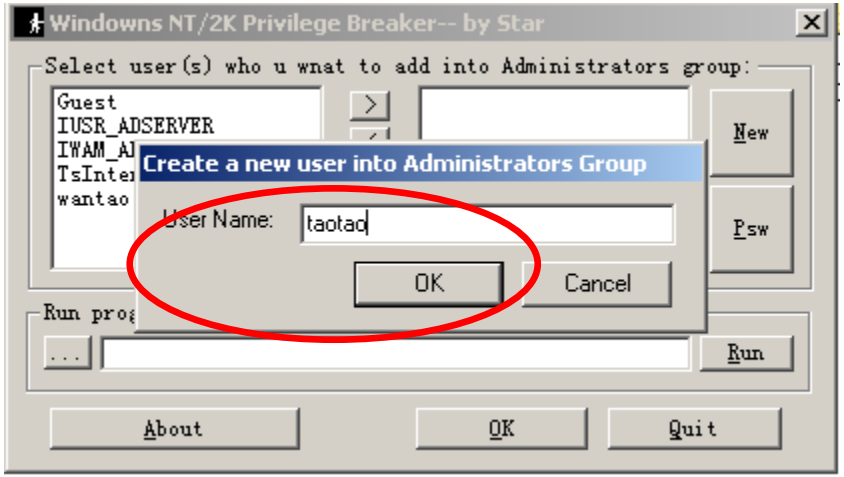
§8.8 物理攻击与防范

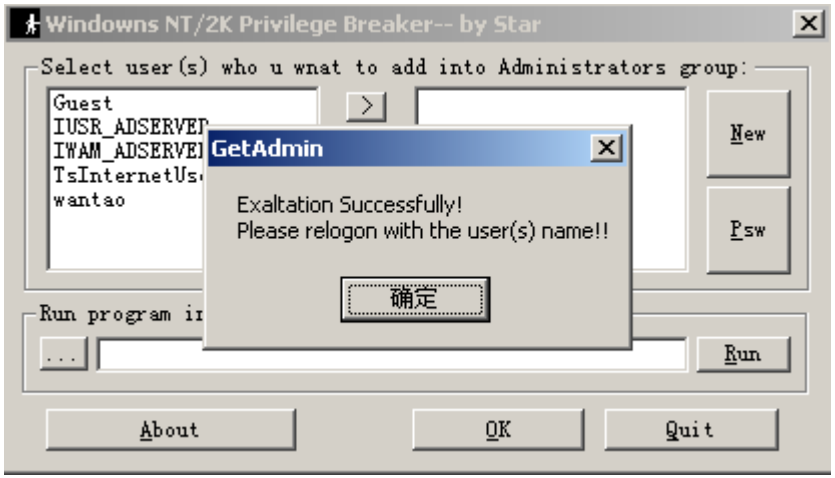
- 提升管理员权限——工具软件GetAdmin.exe
  - 执行GetAdmin.exe，主界面如下



§8.8 物理攻击与防范

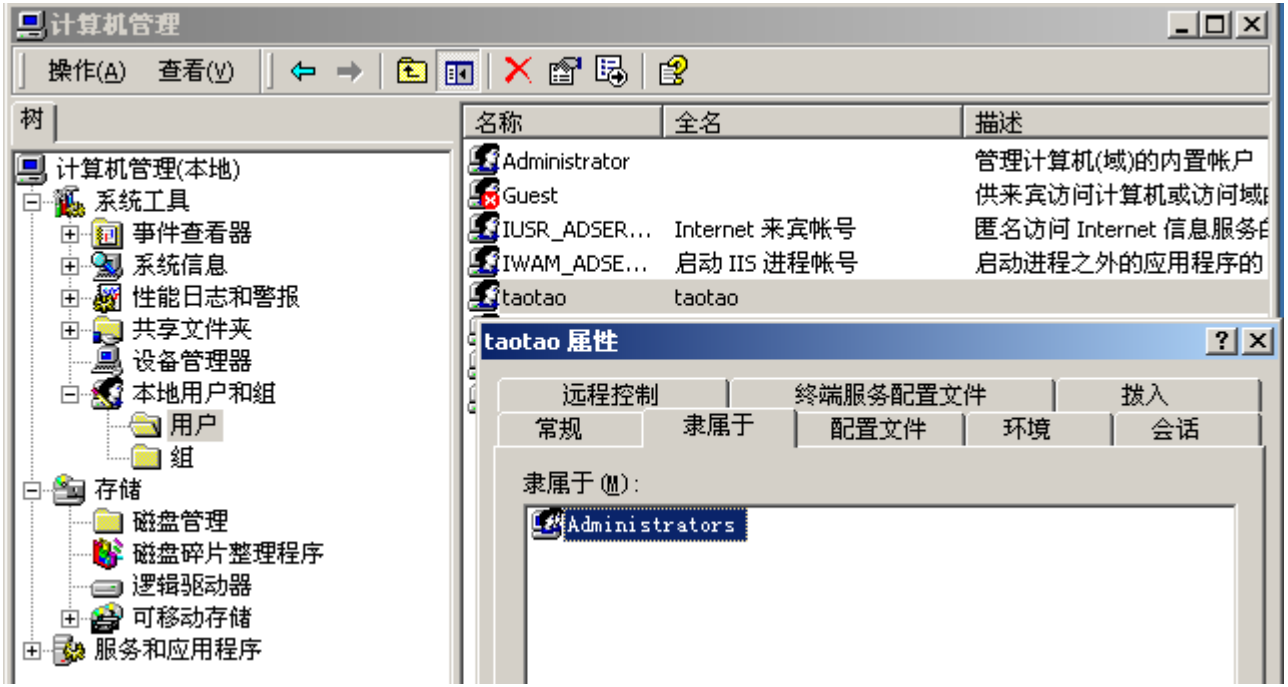
- 提升管理员权限——工具软件GetAdmin.exe





§8.8 物理攻击与防范

- 提升管理员权限——工具软件GetAdmin.exe
  - 查看结果



§8.9 社会工程学攻击

- 社会工程是使用计谋和假情报去获得密码和其他敏感信息的科学，研究一个站点的策略其中之一就是尽可能多的了解这个组织的个体，因此黑客不断试图寻找更加精妙的方法从他们希望渗透的组织那里获得信息。
- 攻击者通过讲述一些似是而非的假话，可以从有权访问的人那里直接得到口令
- 攻击者利用大众的疏于防范的小诡计，让受害者掉入陷阱，盗取身份识别。

§8.9 社会工程学攻击

- 目前社会工程学攻击主要包括两种方式：
  - 打电话请求密码

    尽管不像前面讨论的策略那样聪明，打电话寻问密码也经常奏效。在社会工程中那些黑客冒充失去密码的合法雇员，经常通过这种简单的方法重新获得密码。
  - 伪造Email

    使用telnet黑客可以截取任何一个身份证发送Email的全部信息，这样的Email消息是真的，因为它发自于一个合法的用户。在这种情形下这些信息是绝对的真实。黑客可以伪造这些。一个冒充系统管理员或经理的黑客能较为轻松的获得大量的信息，从而实施他们的恶意阴谋

§8.9 社会工程学攻击

- 例：网络钓鱼、勒索程序
- 网络钓鱼是近来社会工程学的代表应用
- 网络钓鱼方法：
  - 电子 邮件欺诈，冠以中奖、顾问、对账等内容
  - 建立假冒网上银行、网上证券网站，合法网页中插入恶意html代码等
  - 利用虚假的电子商务进行诈骗
  - 利用木马和黑客技术等手段窃取用户信息后实施盗窃活动。
  - 利用用户弱口令等漏洞破解、猜测用户帐户和密码。

§8.9 社会工程学攻击

- 网络钓鱼防范：

（1）针对电子 邮件欺诈。邮件特征：问候语模仿被假冒单位口吻，内容多传递紧迫的信息，索取个人信息，以超低价或海关查没品等为诱饵

（2）针对假冒网上银行、网上证券网站。核对网址；妥善选择和保管密码；做好交易记录；管好数字证书；对异常动态提高警惕；不要通过搜索引擎链接登录支付网关

（3）针对虚假的电子商务信息。特征：交易方式单一，以不发货为由索要余款

（4）其他网络安全防范。安装和升级防火墙和防病毒软件；系统打补丁；不上不了解网站，不执行未经杀毒处理的下载软件；提高自我保护意识

§8.9 社会工程学攻击

假的

- 假的网址列是盖在真的网址列上方
- 网址列并没有跟 IE 窗口对齐



真的

- 网址列与 IE 窗口对齐



- 假的



- 真的

