这是作者的网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您们喜欢，一起进步。前文分享了DNS欺骗（DNS投毒）及钓鱼网站原理知识，并通过Ettercap工具复现某购物网站的钓鱼漏洞。本文将详细讲解木马原理知识，并通过远程服务器IPC $ 漏洞实现木马植入及控制远程服务器。希望这篇基础文章对您有所帮助，更希望大家提高安全意识，学会相关防范，也欢迎大家讨论。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

PS：本文参考了B站（千峰教育feige老师）、安全网站和参考文献中的文章，并结合自己的经验和实践进行撰写，也推荐大家阅读参考文献。

下载地址：https://github.com/eastmountyxz/NetworkSecuritySelf-study

文章目录

前文学习：

[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
[网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
[网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
[网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
[网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
[网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向
[网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨
[网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具
[网络安全自学篇] 九.社会工程学之基础概念、IP获取、IP物理定位、文件属性
[网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码
[网络安全自学篇] 十一.虚拟机VMware+Kali安装入门及Sqlmap基本用法

[网络安全自学篇] 十二.Wireshark安装入门及抓取网站用户名密码（一）
[网络安全自学篇] 十三.Wireshark抓包原理（ARP劫持、MAC泛洪）及数据流追踪和图像抓取（二）
[网络安全自学篇] 十四.Python攻防之基础常识、正则表达式、Web编程和套接字通信（一）
[网络安全自学篇] 十五.Python攻防之多线程、C段扫描和数据库编程（二）
[网络安全自学篇] 十六.Python攻防之弱口令、自定义字典生成及网站暴库防护
[网络安全自学篇] 十七.Python攻防之构建Web目录扫描器及ip代理池（四）
[网络安全自学篇] 十八.XSS跨站脚本攻击原理及代码攻防演示（一）
[网络安全自学篇] 十九.Powershell基础入门及常见用法（一）
[网络安全自学篇] 二十.Powershell基础入门及常见用法（二）
[网络安全自学篇] 二十一.GeekPwn极客大赛之安全攻防技术总结及ShowTime
[网络安全自学篇] 二十二.Web渗透之网站信息、域名信息、端口信息、敏感信息及指纹信息收集
[网络安全自学篇] 二十三.基于机器学习的恶意请求识别及安全领域中的机器学习
[网络安全自学篇] 二十四.基于机器学习的恶意代码识别及人工智能中的恶意代码检测
[网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探
[网络安全自学篇] 二十六.Shodan搜索引擎详解及Python命令行调用
[网络安全自学篇] 二十七.Sqlmap基础用法、CTF实战及请求参数设置（一）
[网络安全自学篇] 二十八.文件上传漏洞和Caidao入门及防御原理（一）
[网络安全自学篇] 二十九.文件上传漏洞和IIS6.0解析漏洞及防御原理（二）
[网络安全自学篇] 三十.文件上传漏洞、编辑器漏洞和IIS高版本漏洞及防御（三）
[网络安全自学篇] 三十一.文件上传漏洞之Upload-labs靶场及CTF题目01-10（四）
[网络安全自学篇] 三十二.文件上传漏洞之Upload-labs靶场及CTF题目11-20（五）
[网络安全自学篇] 三十三.文件上传漏洞之绕狗一句话原理和绕过安全狗（六）
[网络安全自学篇] 三十四.Windows系统漏洞之5次Shift漏洞启动计算机
[网络安全自学篇] 三十五.恶意代码攻击溯源及恶意样本分析
[网络安全自学篇] 三十六.WinRAR漏洞复现（CVE-2018-20250）及恶意软件自启动劫持
[网络安全自学篇] 三十七.Web渗透提高班之hack the box在线靶场注册及入门知识
[网络安全自学篇] 三十八.hack the box渗透之BurpSuite和Hydra密码爆破及Python加密Post请求（二）
[网络安全自学篇] 三十九.hack the box渗透之DirBuster扫描路径及Sqlmap高级注入用法（三）
[网络安全自学篇] 四十.phpMyAdmin 4.8.1后台文件包含漏洞复现及详解（CVE-2018-12613）
[网络安全自学篇] 四十一.中间人攻击和ARP欺骗原理详解及漏洞还原
[网络安全自学篇] 四十二.DNS欺骗和钓鱼网站原理详解及漏洞还原

前文欣赏：

[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入

[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法

[渗透&攻防] 三.数据库之差异备份及Caidao利器

[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

> 声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

一.木马详解

很早之前作者介绍了“Web安全学习路线及木马、病毒和防御初探”，而这篇将结合案例更深入地讲解木马知识，希望对您有所帮助。注意，本文的实验绝对禁止在真实环境中去完成，作者将引用B站视频中虚拟机实验复现，未经授权的测试或攻击行为我们一律禁止。本文仅作为科普文章并提升读者的安全防范意识，关闭远程服务端口。

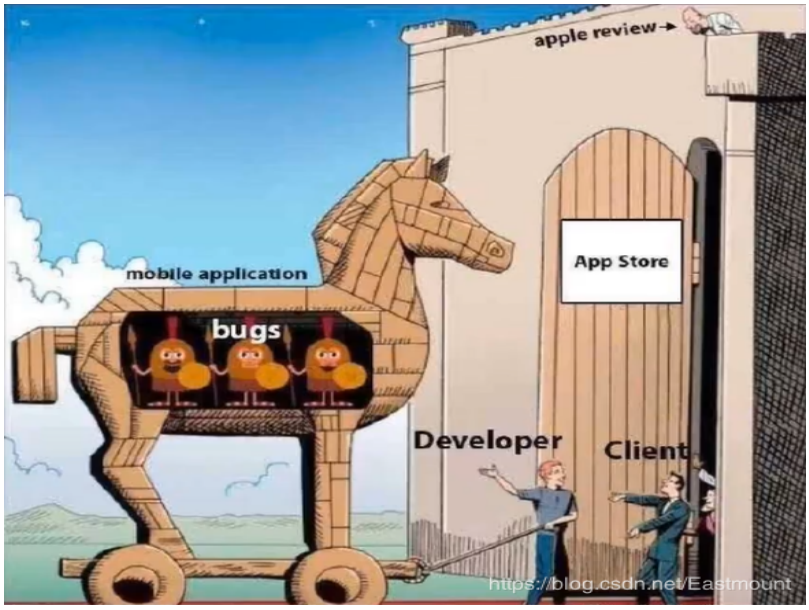
实训目标：

通过经典的木马攻击还原场景，来学习木马的制作，并实现植入木马对目标主机进行完全控制。现实中，木马发送给目标有很多种方法，比如发送垃圾邮件、点击垃圾链接、访问HS网站、从非官方网站下载软件等，并且很多人在中木马之后还不知道。本篇文章的实验主要是针对服务器的木马植入展开。

特洛伊木马：

比喻侵入内部的破坏性因素。来源于希腊神话中特洛伊战争，特洛伊人劫持了希腊最美的女人海伦，古希腊为了夺回海伦，发动了对特洛伊的远征，围困十年之久，但就是攻不下这个城池，最后希腊人建造了一个强大的木马（木头做的马），让希腊武士藏在木马中，然后假装撤兵，特洛伊人把这个木马当作战利品，晚上希腊武士趁其熟睡打开城门攻城。现在计算机病毒也命名为特洛伊木马，它会想方设法植入目标，从内部瓦解对方。

- 木马通常称为黑客程序、恶意代码，也称为特洛伊木马
- 基于远程控制的黑客工具



木马的特性：

- 隐蔽性
- 潜伏性
- 再生性

木马的组成：

- 客户端程序
  客户端程序是安装在攻击者（黑客）方的控制台，它负责远程遥控指挥，比如黑客需要数据则控制远程恶意代码或木马程序去搜集数据
- 服务端程序
  服务器端程序即是木马程序，它被隐藏安装（植入）在被攻击（受害）方的电脑上，目标主机也称为肉鸡

木马的危害：

- 盗取用户信息，比如网游账户、网银信息、QQ密码等。QQ密码虽然加密，但输密码时可以通过键盘记录发送给客户端
- 传播病毒
- 占用系统资源，降低电脑效能
- 将本机作为工具来攻击其他设备等

中了木马的征兆：

- 硬盘不停的读写

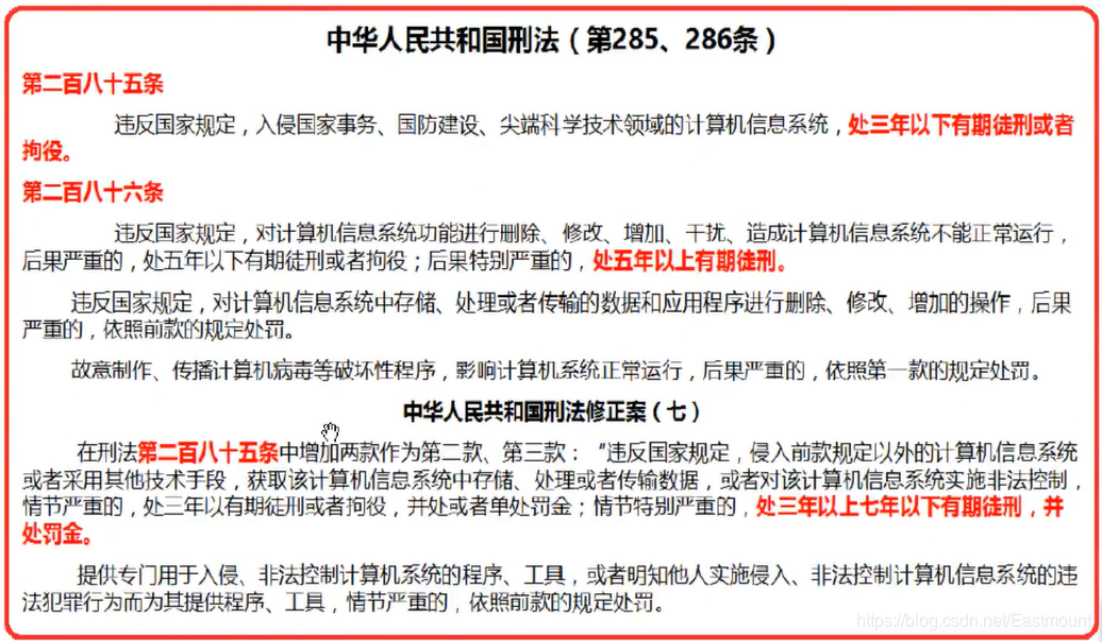
- 鼠标键盘不停使唤
- 窗口突然被关闭
- 新的窗口莫名其妙地打开

木马传播途径：

- 网页浏览时利用浏览器漏洞或浏览器插件（Flash、迅雷等）漏洞
- 通过QQ、MSN等及时通讯软件，发送恶意网址链接或木马病毒文件
- 使用U盘等移动存储介质。电脑别轻易插入不认识人的U盘，社会工程学会利用人性贪婪瓦解内部防火墙
- 打开陌生的邮件，通过电子邮件内恶意代码或含木马病毒的附件
- 伪装成多媒体影音文件或植入木马的应用软件，利用P2P平台和网址传播
- 利用操作系统漏洞或弱口令直接远程植入
- 下载来源不明的程序

如何防御：

- 提高警惕性，别占小便宜，别点击垃圾链接或邮件
- 从官网下载程序，密码设置复杂
- 设置防火墙和杀毒软件，定期杀毒并清理电脑
- 防止社会工程学诱骗或攻击



中华人民共和国刑法（第285、286条）

第二百八十五条

违反国家规定，入侵国家事务、国防建设、尖端科学技术领域的计算机信息系统，**处三年以下有期徒刑或者拘役。**

第二百八十六条

违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰、造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，**处五年以上有期徒刑。**

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

中华人民共和国刑法修正案（七）

在刑法**第二百八十五条**中增加两款作为第二款、第三款："违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，**处三年以上七年以下有期徒刑，并处罚金。**

提供专门用于入侵、非法控制计算机系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

二.木马实验

1.实验环境

环境介绍：

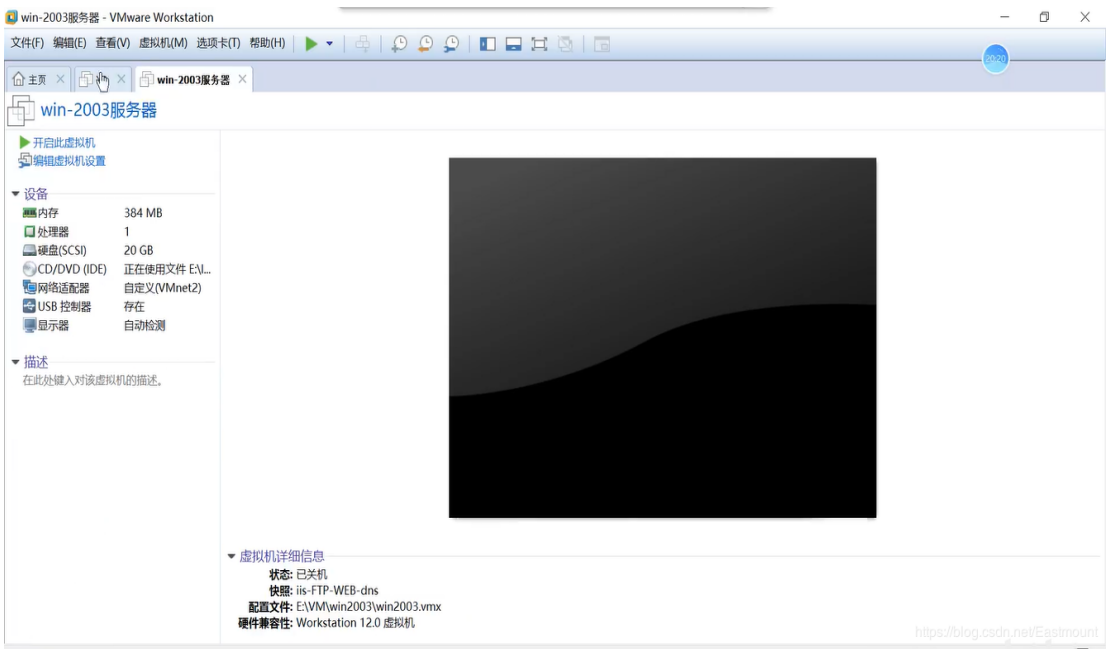
- 虚拟机软件：VMware V12.0版本
- 虚拟机：Windows XP（模拟黑客攻击机）、Windows Server 2003（模拟被木马控制方）
- 黑客工具：HGZ软件、NTscan

实验流程：

1.开启虚拟机，将xp和2003桥接到VMnet1上
2.配置IP地址并测试网络连通性：XP配置IP为10.1.1.1/24、2003配置IP为10.1.1.2/24
3.制作木马：使用HGZ制作木马，并将木马生成在D盘
4.IPC $ 暴力爆破密码
5.与目标主机建立IPC $
6.植入木马到目标主机
7.设置目标主机运行木马
8.成功控制目标主机

2.配置网络

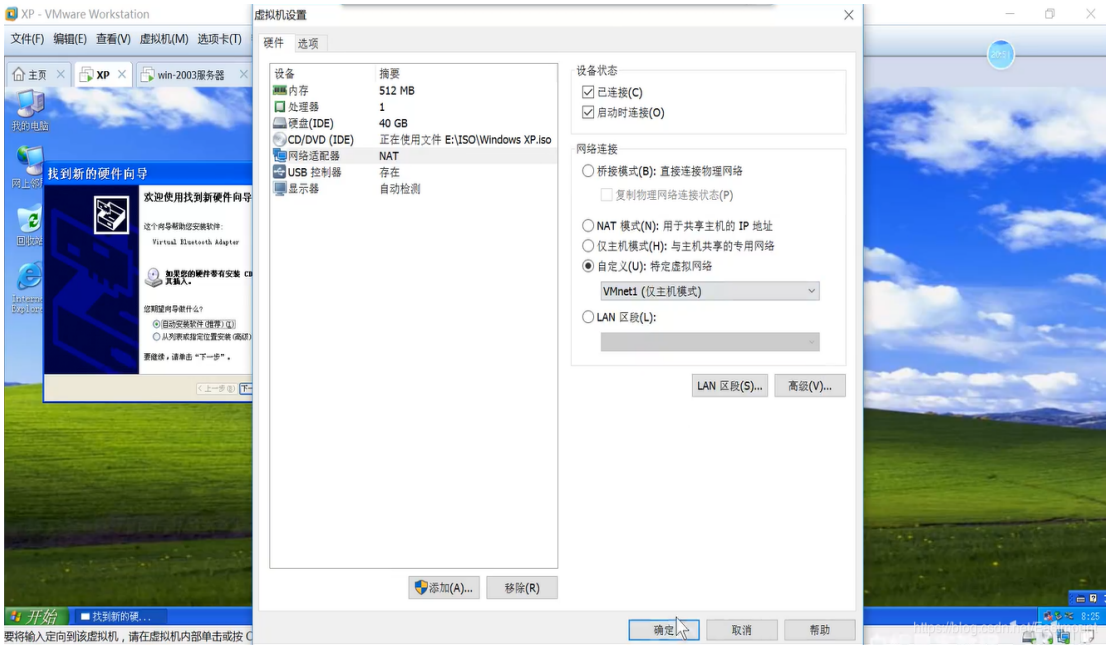
第一步，开启两台虚拟机。

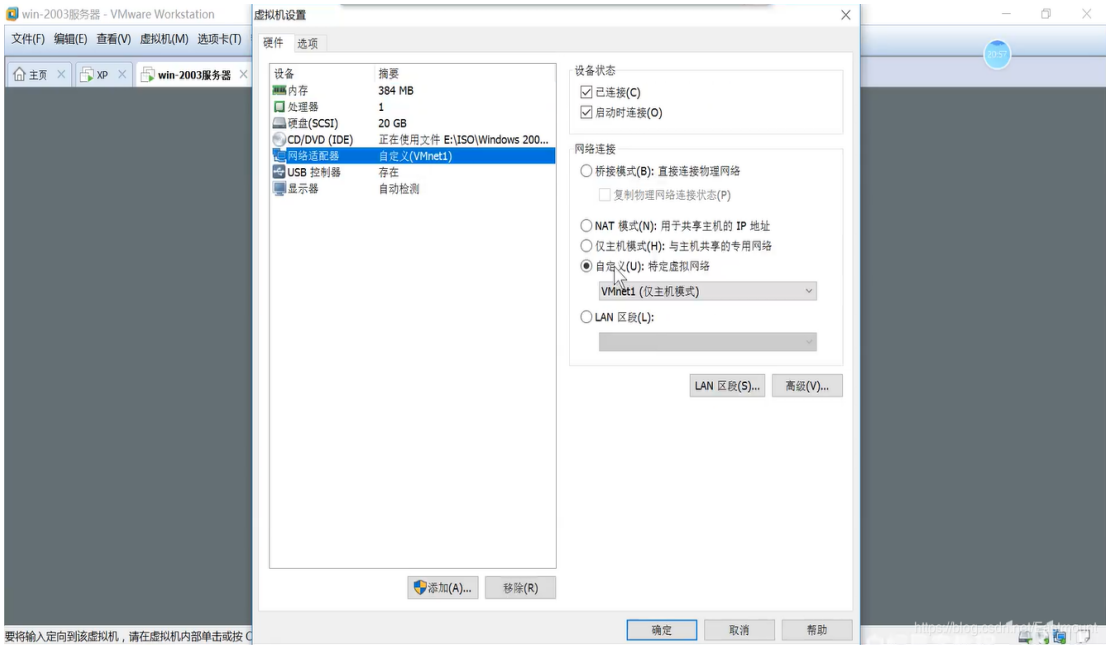


使用还原快照如下图所示：

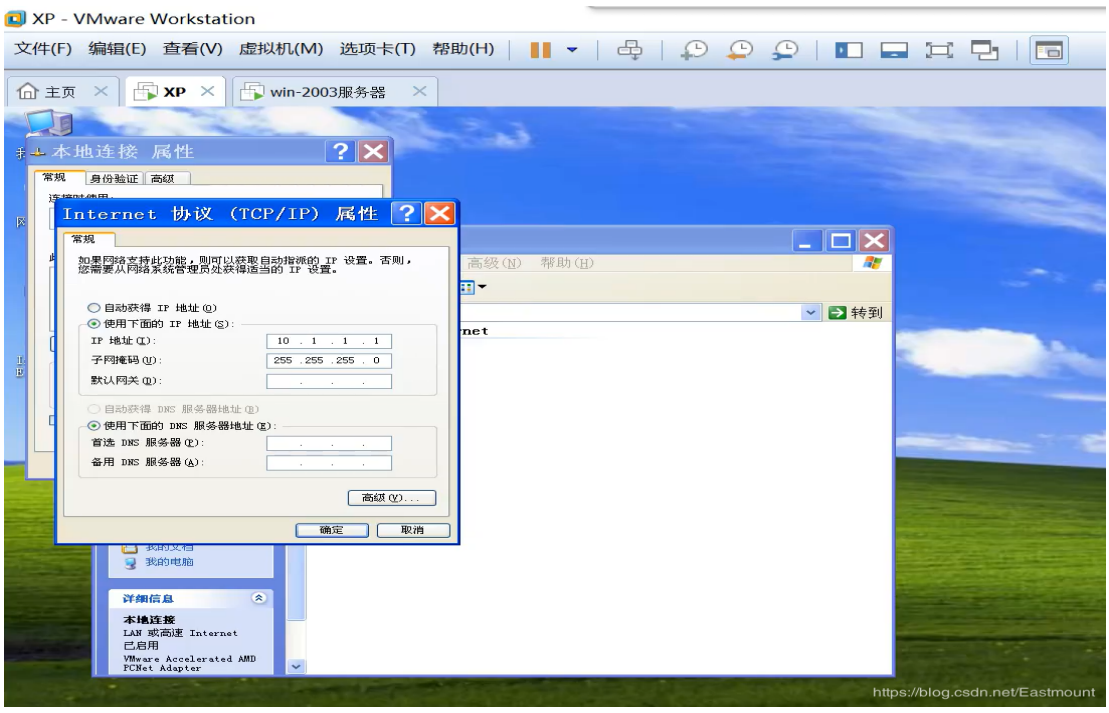
第二步，桥接网络。

XP和2003系统均设置为VMnet1网络。

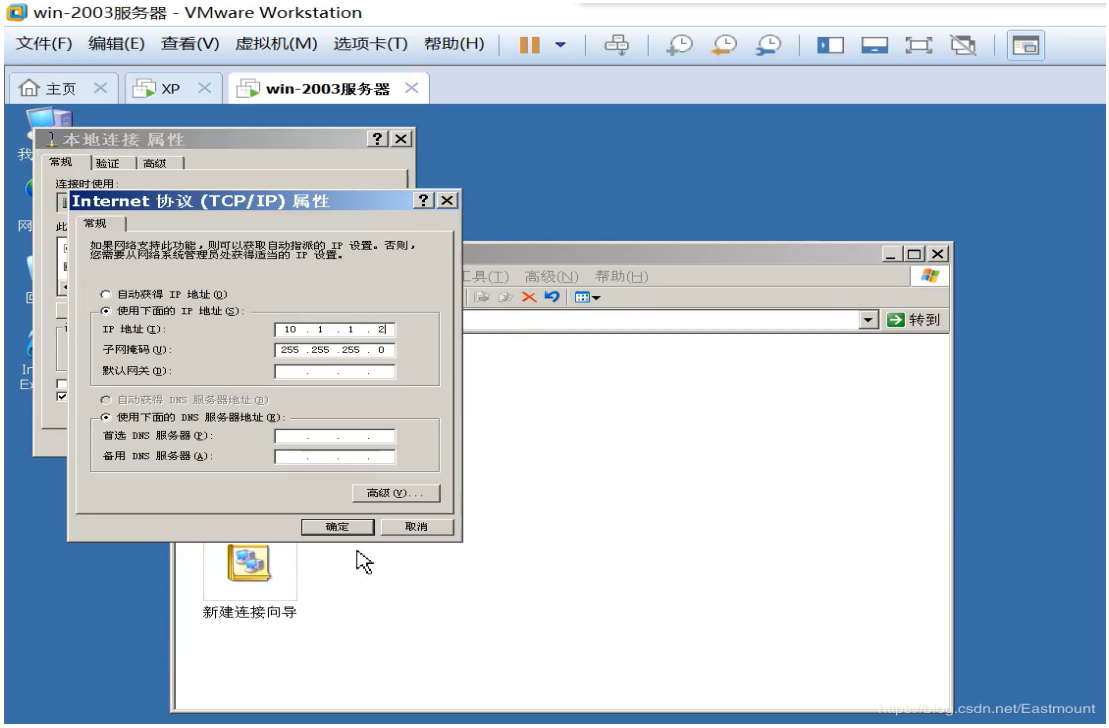




接着配置IP地址，Windows XP系统IP地址配置为10.1.1.1。



Windows Server 2003配置IP地址为10.1.1.2

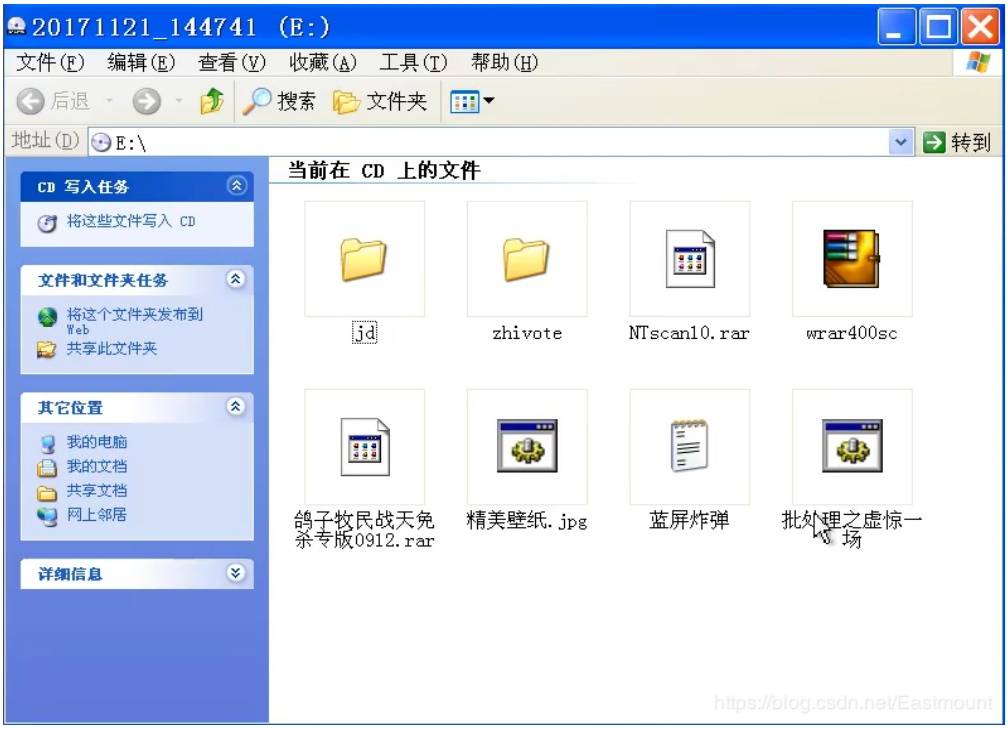


尝试ping 10.1.1.2 -t，当网络建立好之后，我们开始制作木马。

3.制作木马

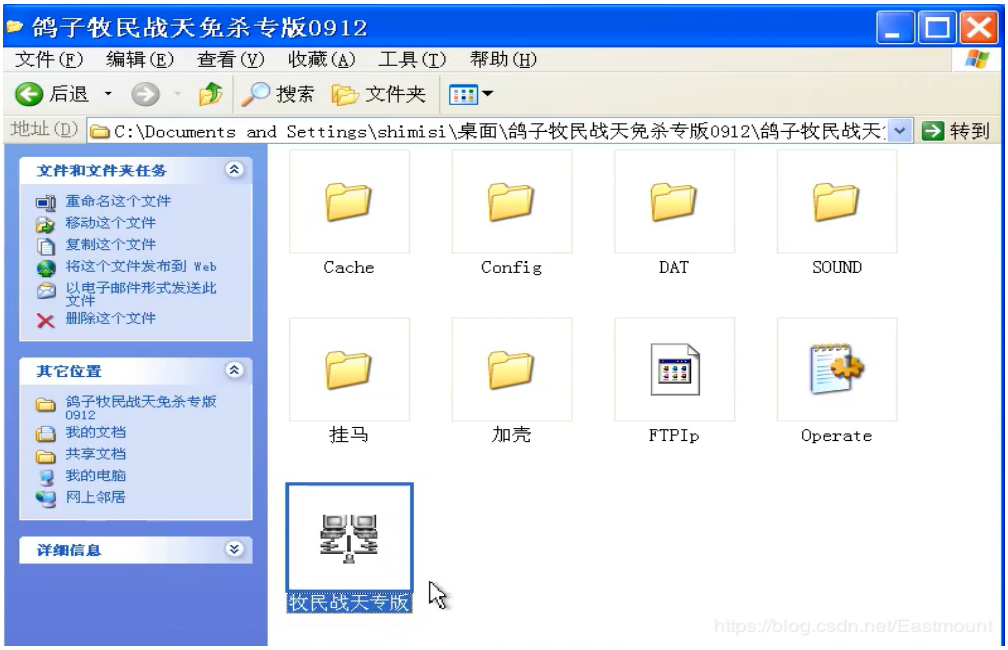
第一步，制作木马。

使用HGZ制作木马。

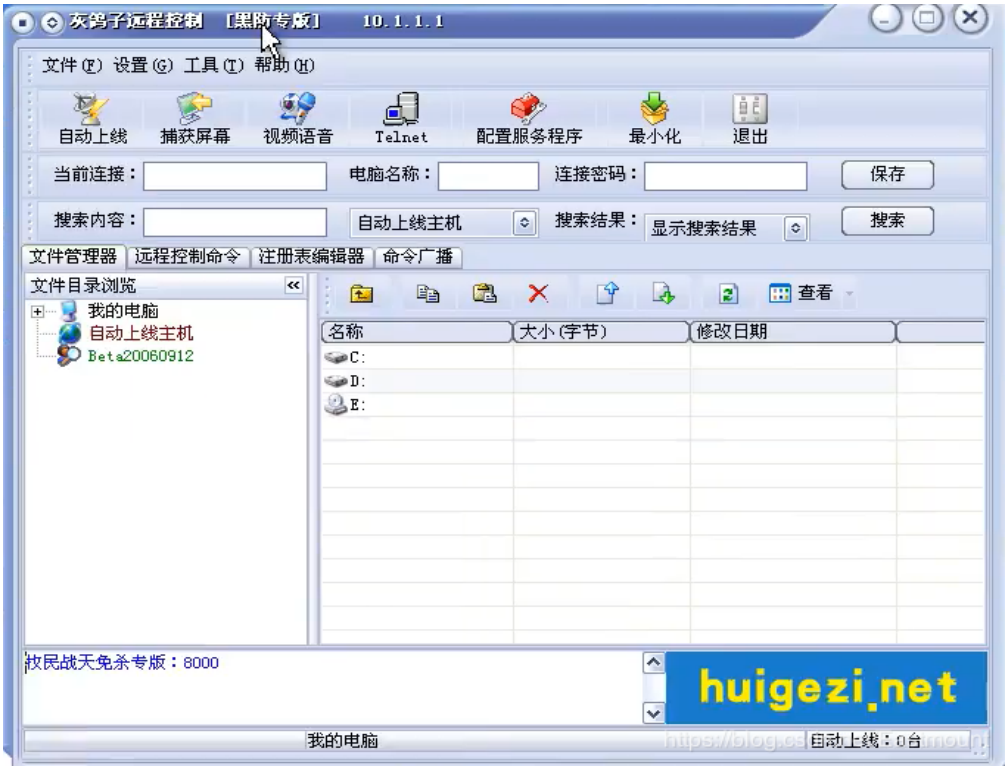


首先我们解压HGZ压缩包，如下图所示。

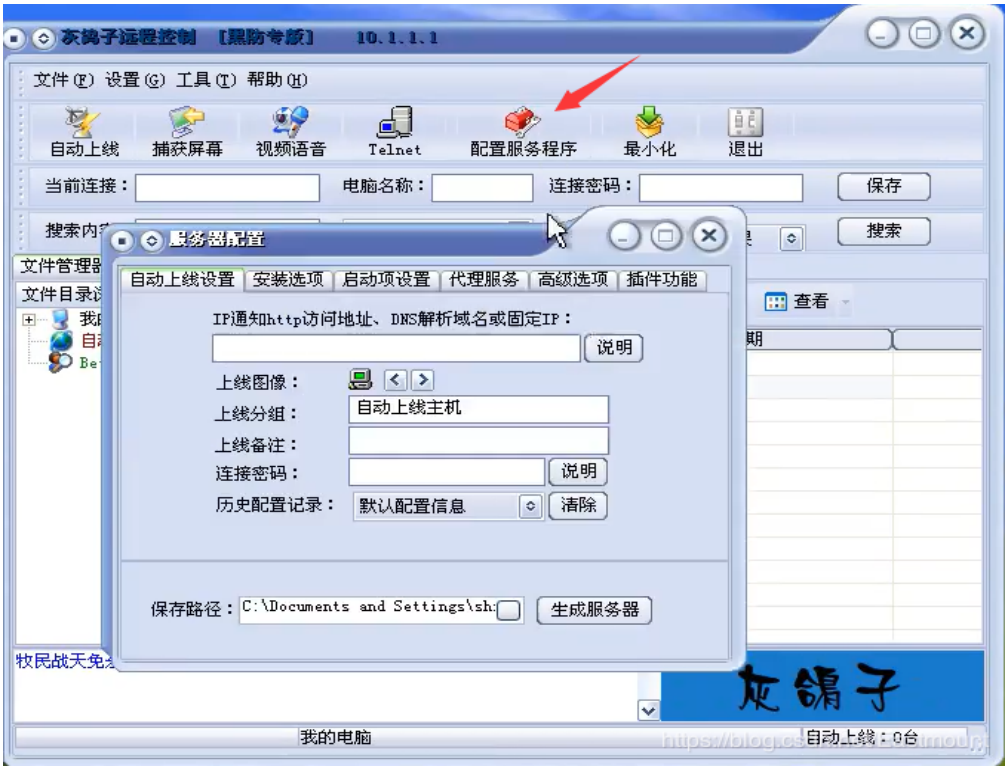
解压之后如下图所示：



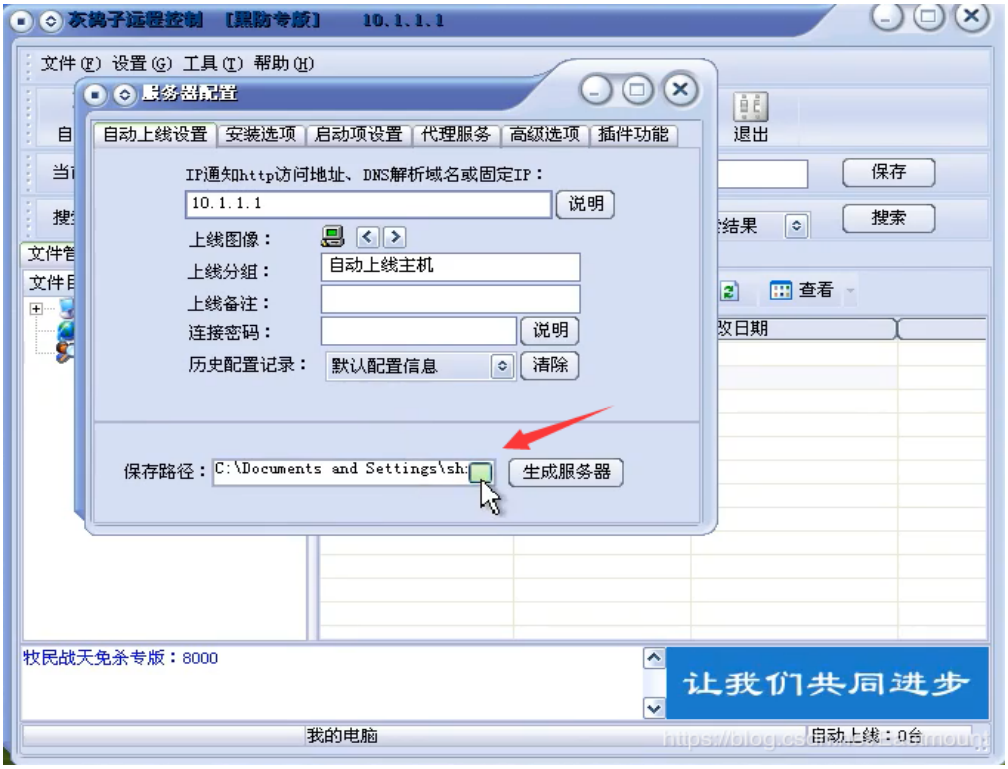
HGZ软件运行如下图所示。左边显示自动上线主机（肉鸡），凡是中木马的肉鸡都会自动上线，木马会主动连接控制方并请求被完全控制。



首先我们需要生成木马，点击“配置服务程序”生成木马。

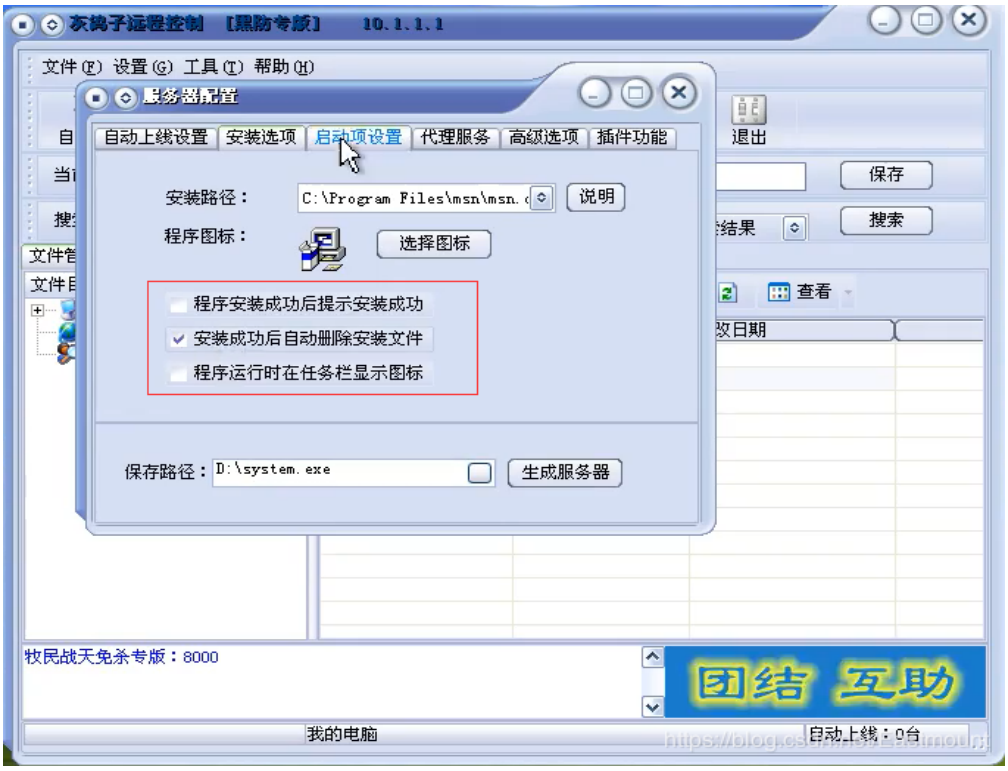


IP通常是黑客电脑的IP地址，因为生成的木马需要植入目标，它会自动连接黑客并发送信息，故填写“10.1.1.1”地址。接着点击底部的方块，选择所制作木马的保存路径。

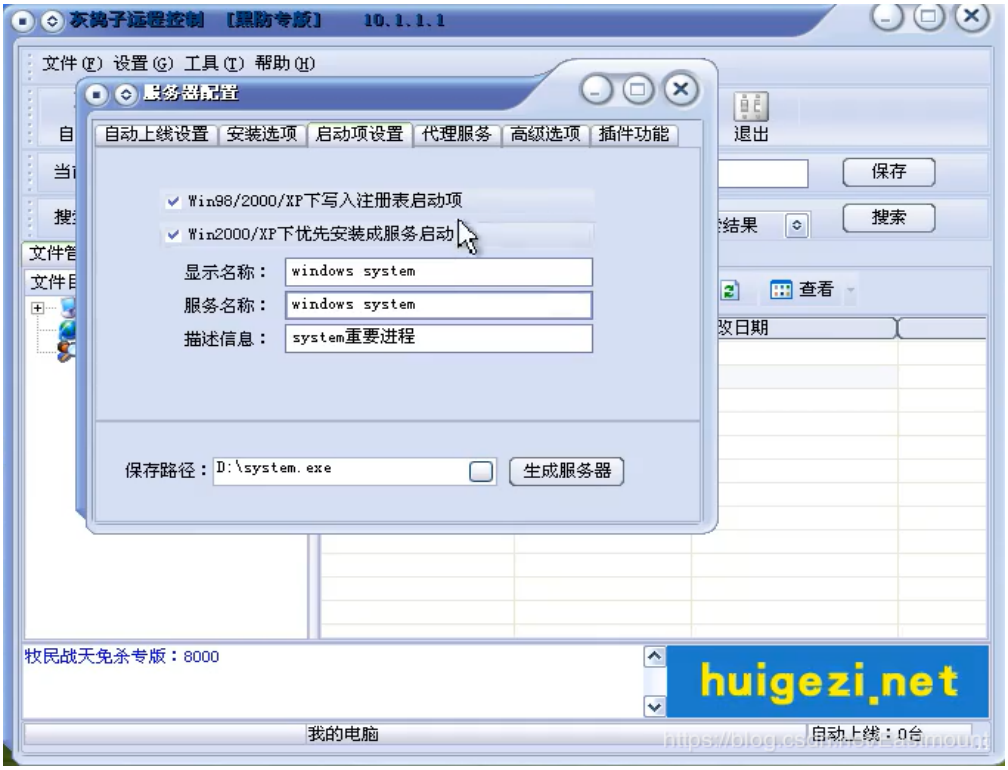


存储至D盘，并且命名为system，尽量和真实的名称类似，其隐蔽性更高。

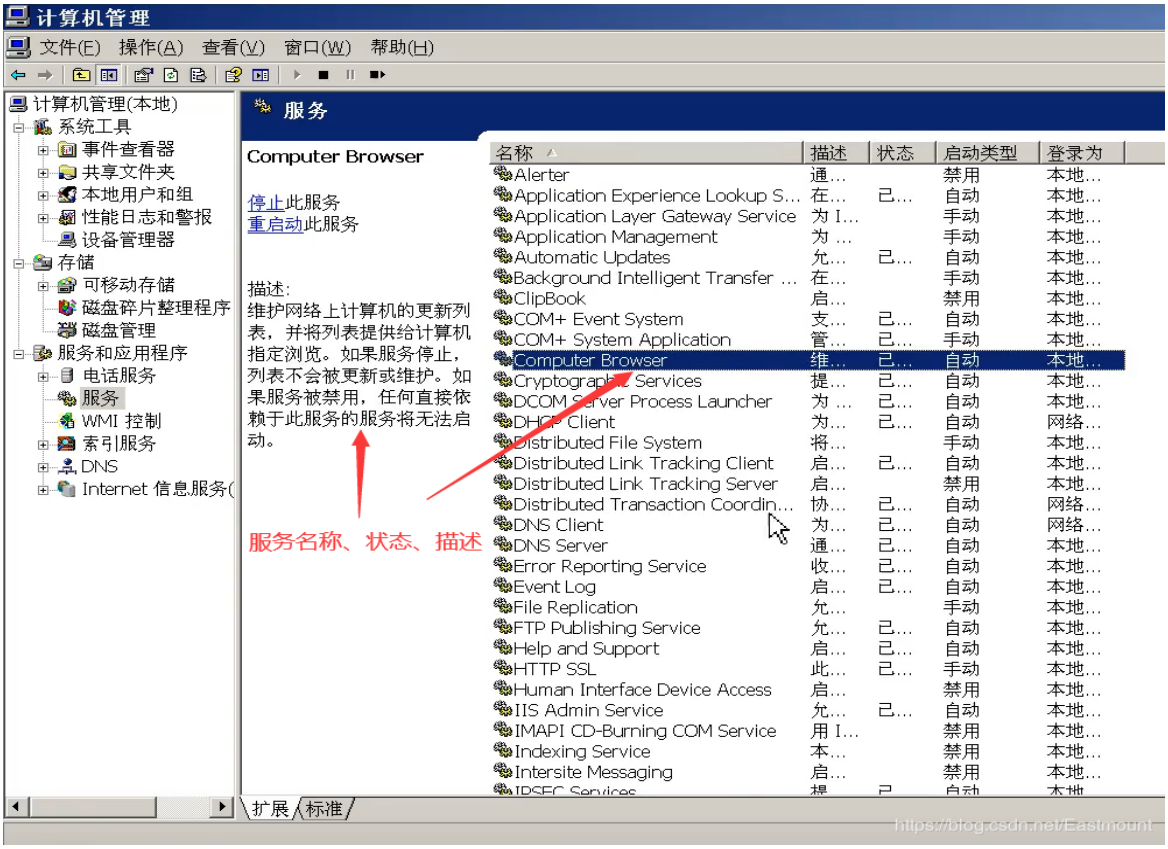
在“安装选项”中，只勾选“安装成功后自动删除安装文件”选项，切勿勾选提示安装成功和运行显示图标。



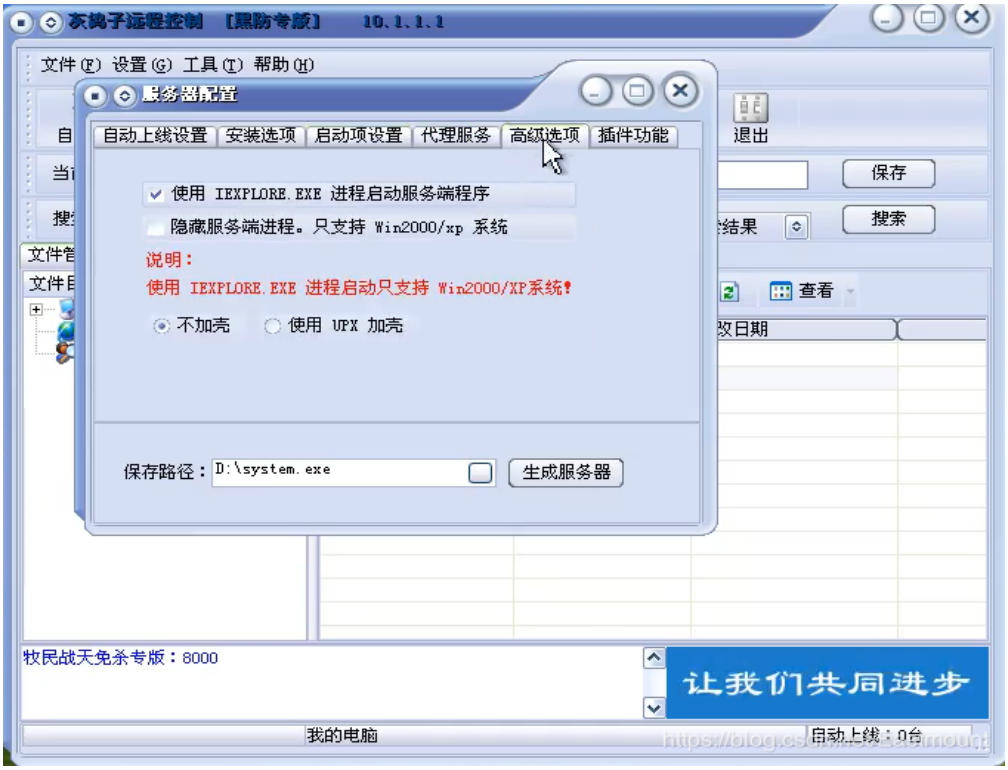
为什么木马比较难找？因为我们会将木马服务名称和描述修改，伪装成正常程序所运行的服务。比如服务名称修改为“windows system”，描述信息修改为“system重要进程”。



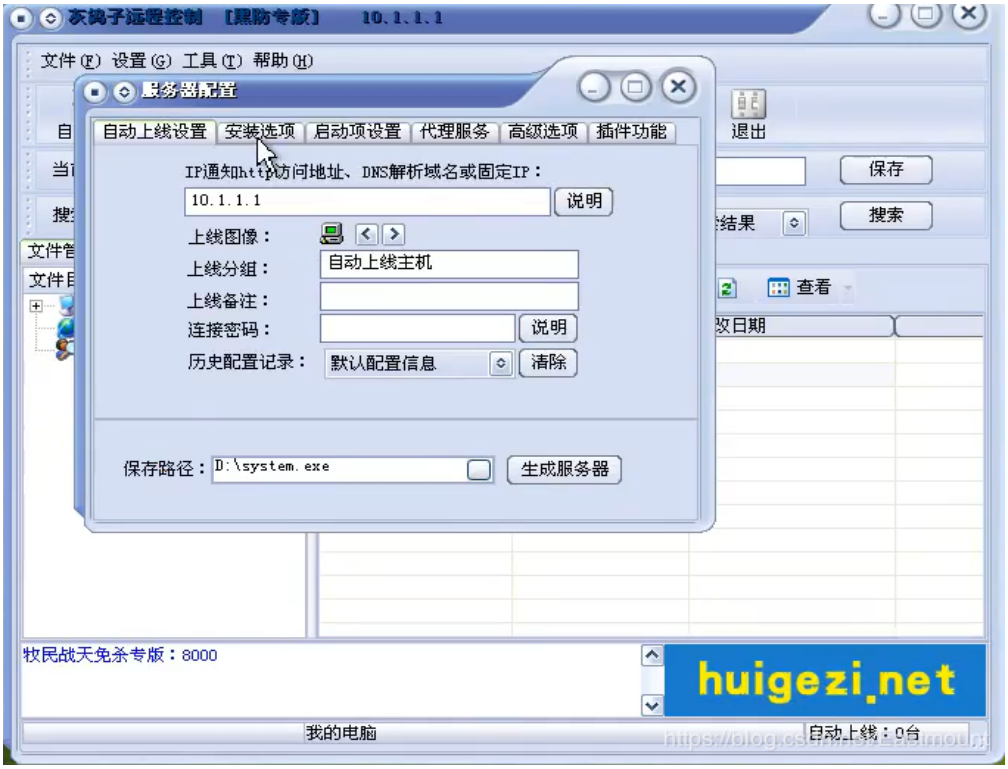
本地服务查找如下图所示：



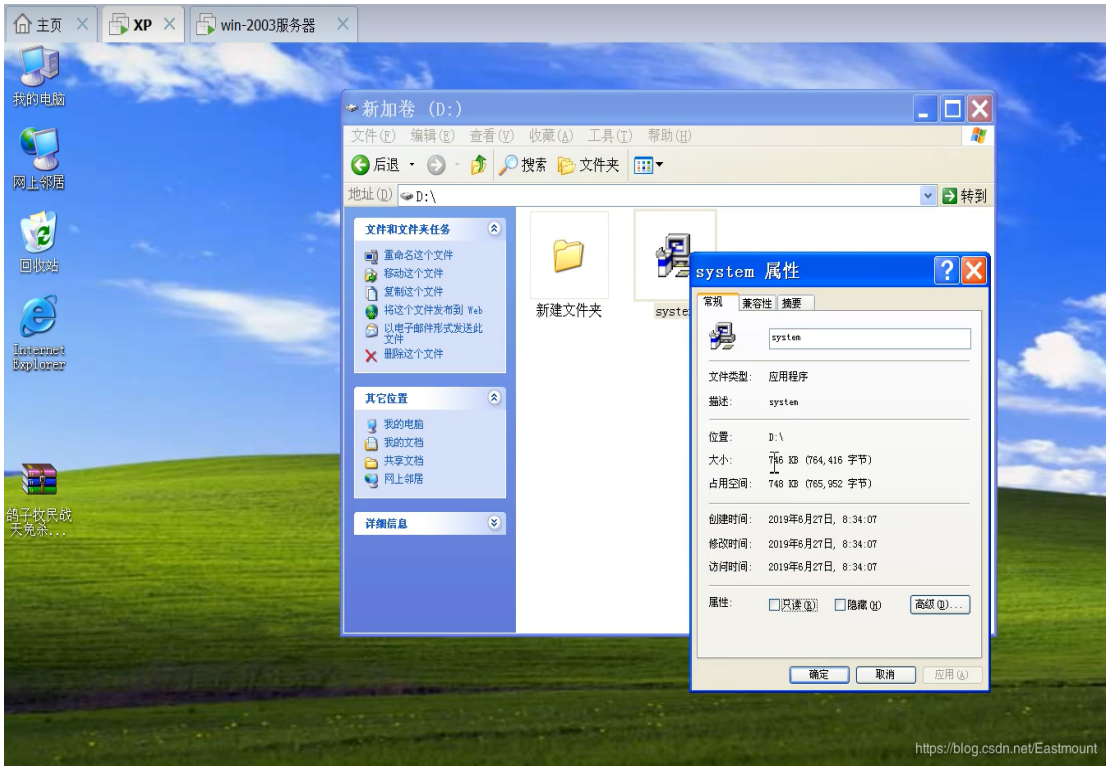
高级选项可以将木马伪装成“IEXPLORE.EXE”进程。



最后点击“生成服务器”，成功制作木马。



可以在D盘看到生成的木马。



4.植入木马

接下来我们需要植入木马并自动运行，主要包括4个步骤：

- IPC $ 暴力爆破
- 与目标主机建立IPC $
- 植入木马到目标主机
- 设置目标主机运行木马

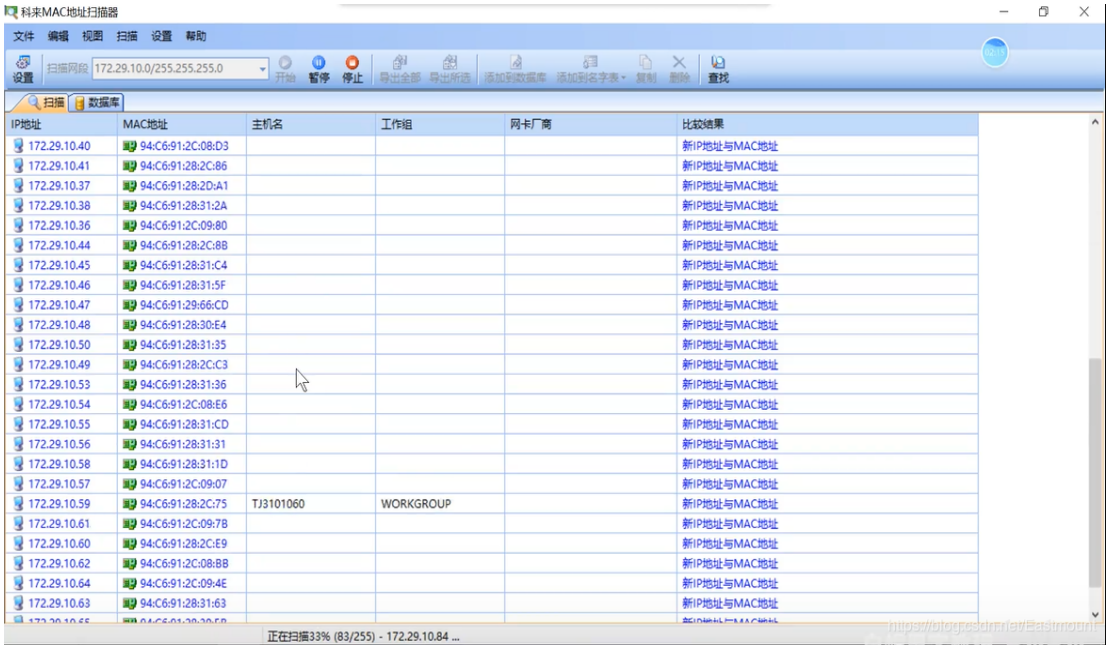
其基本思路是希望对方能运行木马，但运行前需要将木马植入到目标主机上，那么如何植入呢？在未经授权情况很难将木马拷贝到别人的电脑上。这里需要利用IPC $漏洞，调用445端口号实现。445端口中有个IPC $ ，称之为空连接，没有固定文件夹的共享；而C$ 、D$ 、E$ 代表分区共享，是有固定文件夹的。换句话说，445端口打开就相当于我们可以在局域网中轻松访问各种共享文件夹，如果您的电脑是弱密码，很容易就被攻破，这里使用IPC $ 暴力爆破。

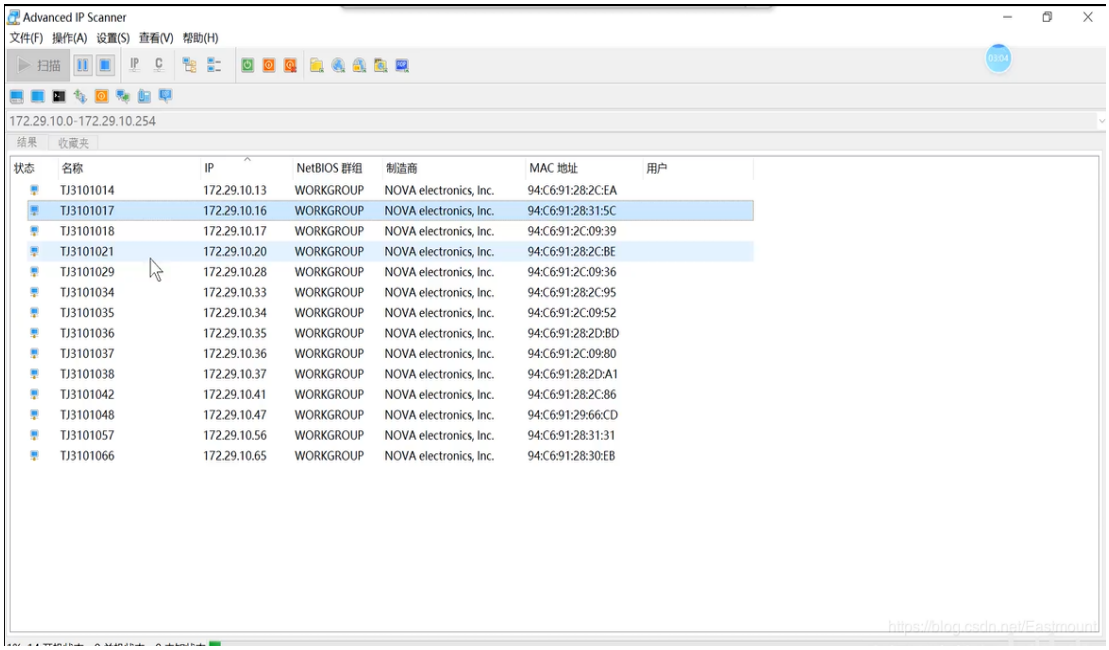
补充1：
IPC $ 暴力爆破是有条件的，就是别人有服务接口，比如对方开了FTP服务。hydra工具是出名的暴力爆破工具，之前的文章“三十八.hack the box渗透之BurpSuite和Hydra密码爆破及Python加密Post请求（二）”也讲述过。Web渗透之前通常需要扫描IP地址和开启的端口号、服务等，信息收集的方法有很多，通过收集发现目标开启的接口，接着才是通过暴力爆破获取最后的密码。

> **445端口**
> 该端口是一个毁誉参半的端口，有了它我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机，他们能通过该端口偷偷共享你的硬盘，甚至会在悄无声息中将你的硬盘格式化掉。2017年10月，由于病毒“坏兔子”来袭，国家互联网应急中心等安全机构建议用户及时关闭计算机以及网络设备上的445和139端口。勒索病毒也与445端口号相关。
>
> **如何预防呢?**
> 关闭该服务端口，或配置高级防火墙且屏蔽任何人访问445。
>
> **IPC$(Internet Process Connection)**
> IPC$ 是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。IPC $ 是NT2000的一项新功能，它有一个特点，即在同一时间内，两个IP之间只允许建立一个连接。NT2000在提供了 IPC $ 功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(C$ 、D$ 、E$ …)和系统目录(C:\windows)共享。所有的这些初衷都是为了方便管理员的管理。但好的初衷并不一定有好的收效，一些别有用心者会利用IPC$访问共享资源，导出用户列表，并使用一些字典工具，进行密码探测。

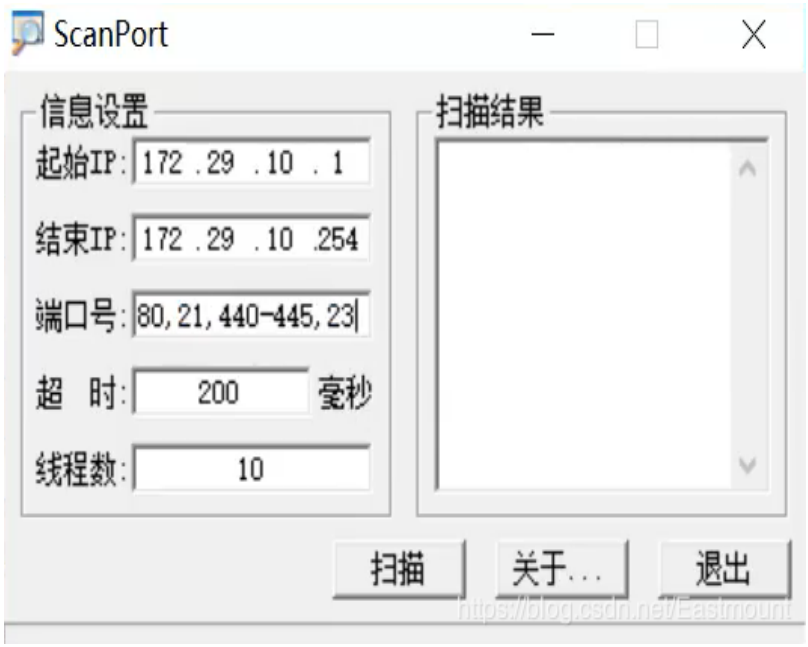
接着开始讲解具体的操作。

第一步，收集信息再进行暴力爆破。
通过扫描软件收集信息，其原理是发送ping请求判断其是否在线，先扫描IP地址。推荐前文：
[网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具
[网络安全自学篇] 二十二.Web渗透之网站信息、域名信息、端口信息、敏感信息及指纹信息收集





当服务器IP地址确定之后，我们还可以扫描开放的端口号。软件包括Nmap、ScanPort等。



简单总结： 首先扫描IP地址，接着扫描开放的端口，比如80端口、21端口、445端口等。如果开放80端口，可以通过软件（如Acunetix Web Vulnerability Scanner）进一步扫描网页漏洞，属于服务类漏洞；如果攻击445端口或21端口，则属于系统类攻击。确定漏洞之后，我们需要进一步利用漏洞进行Web渗透。

第二步，调用命令访问共享。

输入如下命令进行共享访问，它会提示您输入登录账号和密码。

```
net use \\10.1.1.2\ipc$
```

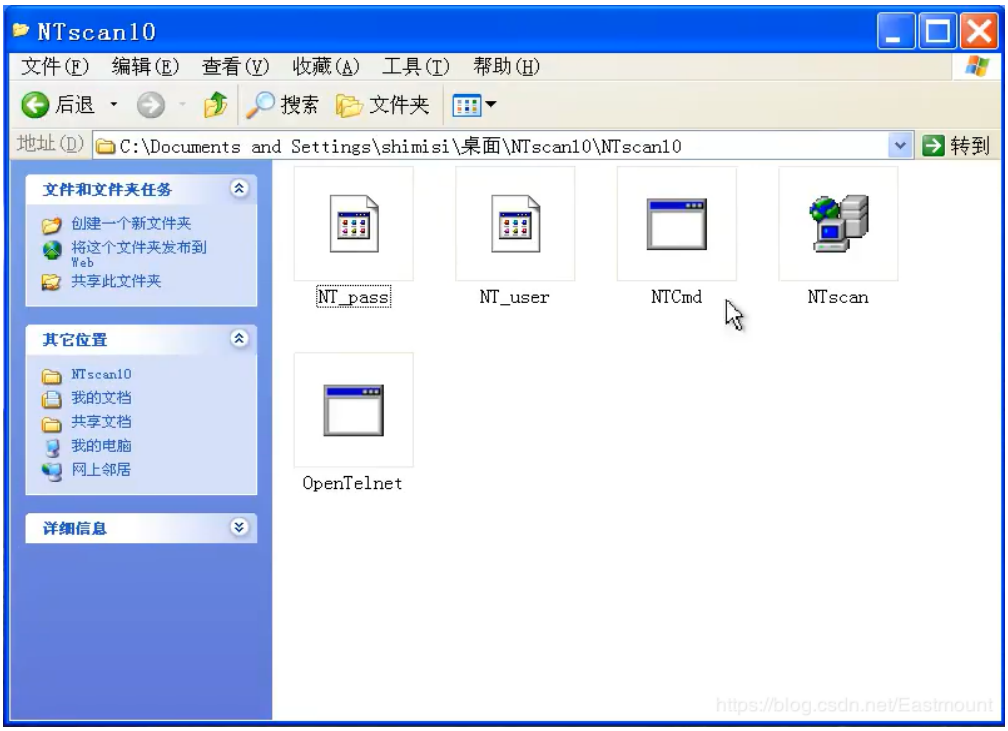
```
C:\Documents and Settings\shimisi>net use \\10.1.1.2\ipc$
密码或用户名在 \\10.1.1.2\ipc$ 无效。

为 '10.1.1.2' 输入用户名: feifei
输入 10.1.1.2 的密码:
发生系统错误 1326。

登录失败: 未知的用户名或错误密码。


C:\Documents and Settings\shimisi>
```

返回结果提示“登录失败：未知的用户名或错误密码”，接下来怎么办呢？我们只能进行暴力爆破。

第三步，使用NTscan软件暴力爆破，该软件支持远程连接IPC $和利用字典文件。

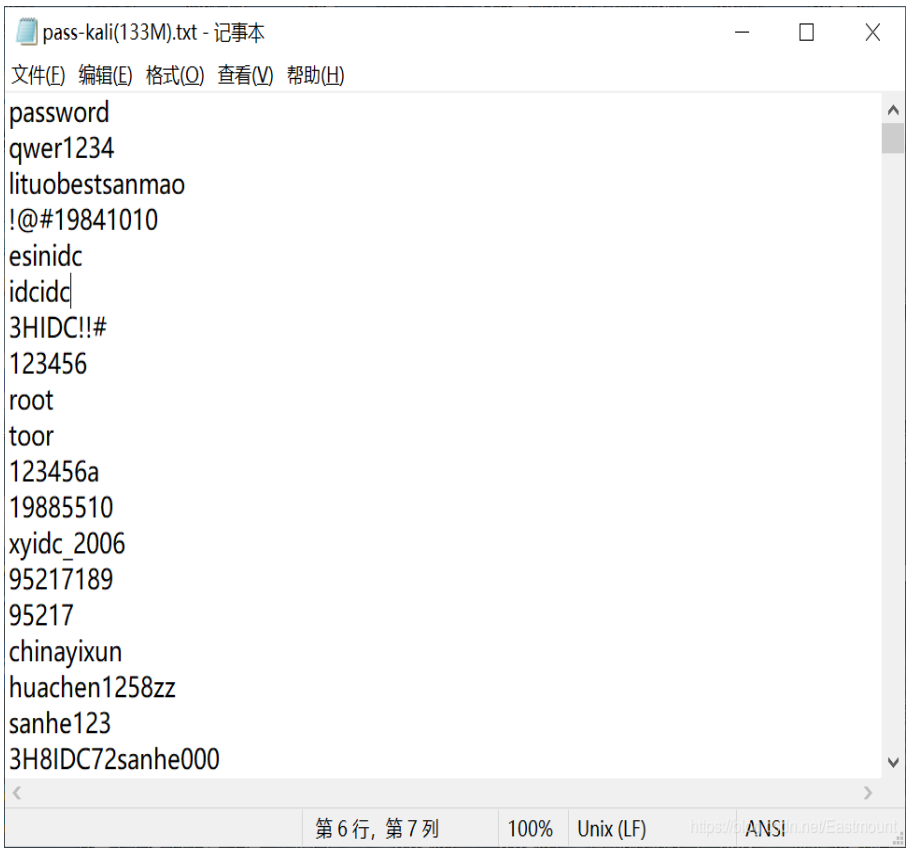
字典文件为“NT_pass”（密码）和“NT_user”（用户名），小的字典有几KB、几兆的，大的字典有上TB的。服务器用户名通常会设置为administrator、Admin等，如果您是网站

管理员，建议将服务器的用户名和密码修改，而且服务器一定要设置密码且不为弱密码（长度限制、大小字母数组特殊符号组成）。

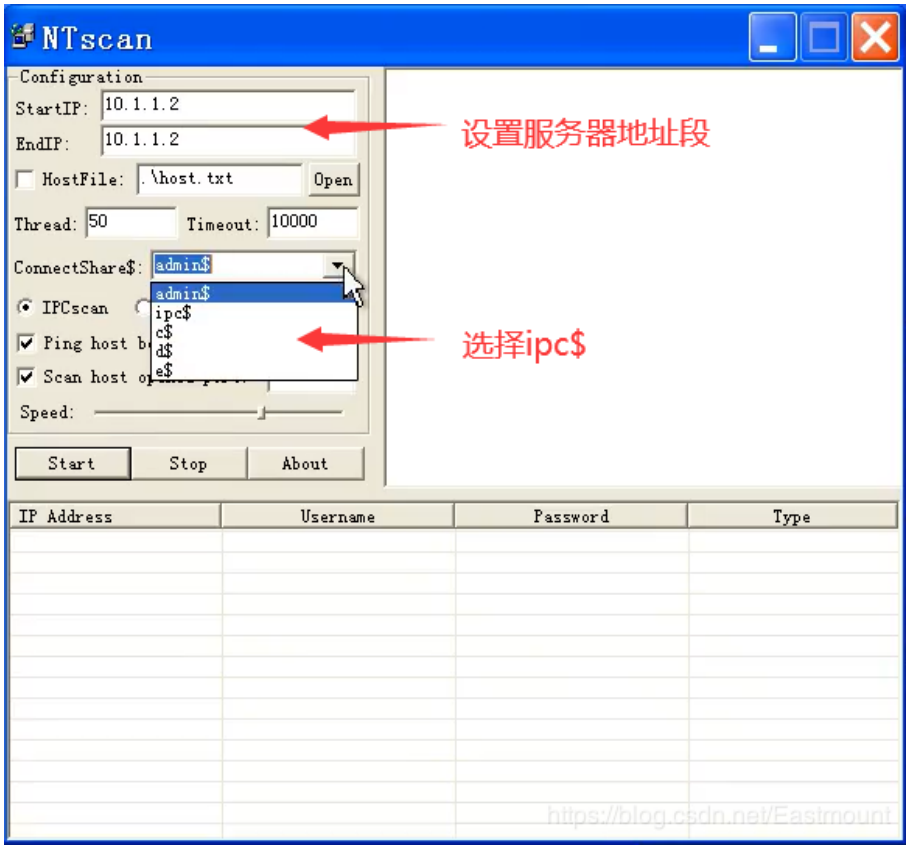


字典文件通常包括一些弱密码，包括空密码、弱密码、常用密码、公司名称、公司符号或缩写、客户信息、老板生日等。下图仅展示了简单的密码，如“123456”、“password”、“%null%”等。

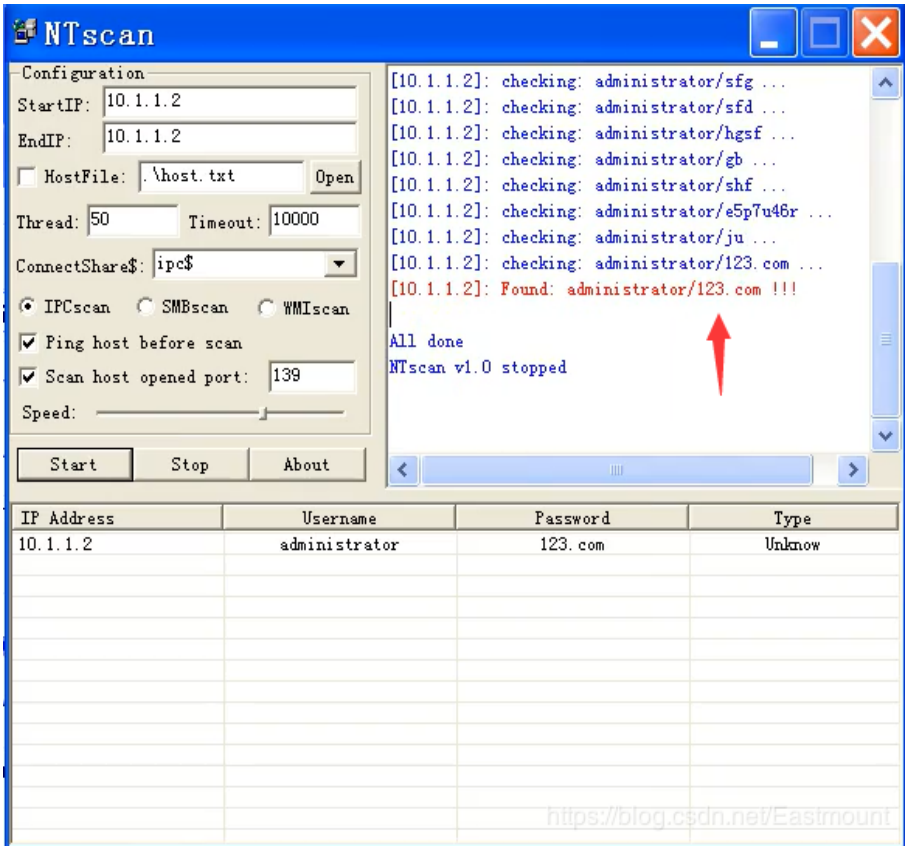
真实的字典会很大，比如作者133MB的密码字典文件，可用于暴力爆破，网络安全工程师，通常都有属于自己的密码字典文件、目录扫描字典文件等。



接着运行软件，输入IP地址“10.1.1.2”，选择IPCsan连接共享“IPC $”。



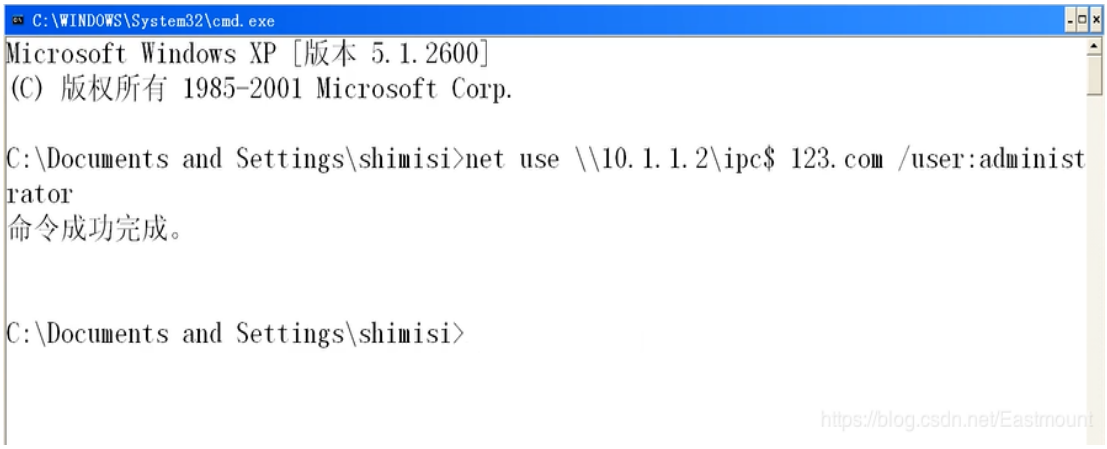
点击“Start”开始扫描，成功获取了密码“123.com”，如下图所示。



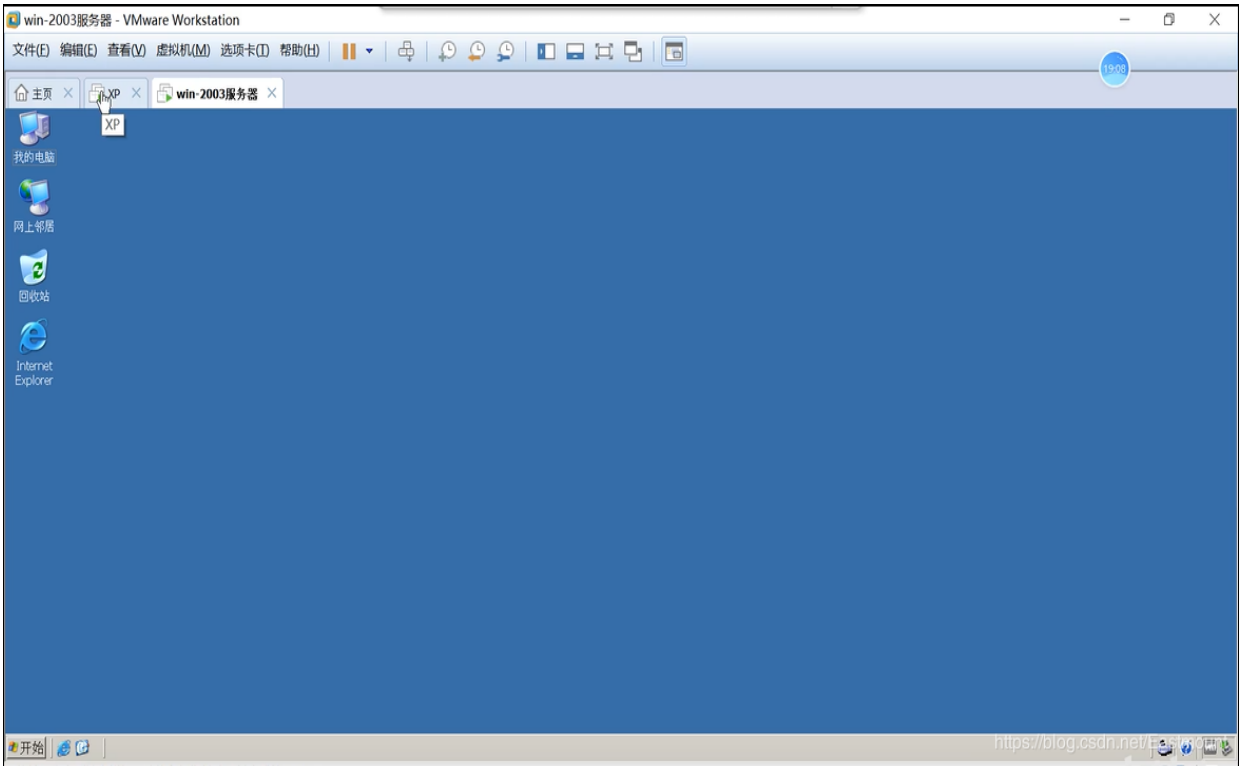
第四步，与目标主机建立IPC $ 空连接。

远程连接输入用户名和密码。

```
net use \\10.1.1.2\ipc$ 123.com /user:administrator
```



此时，服务器被连接之后它是没有反应的，如下图所示。

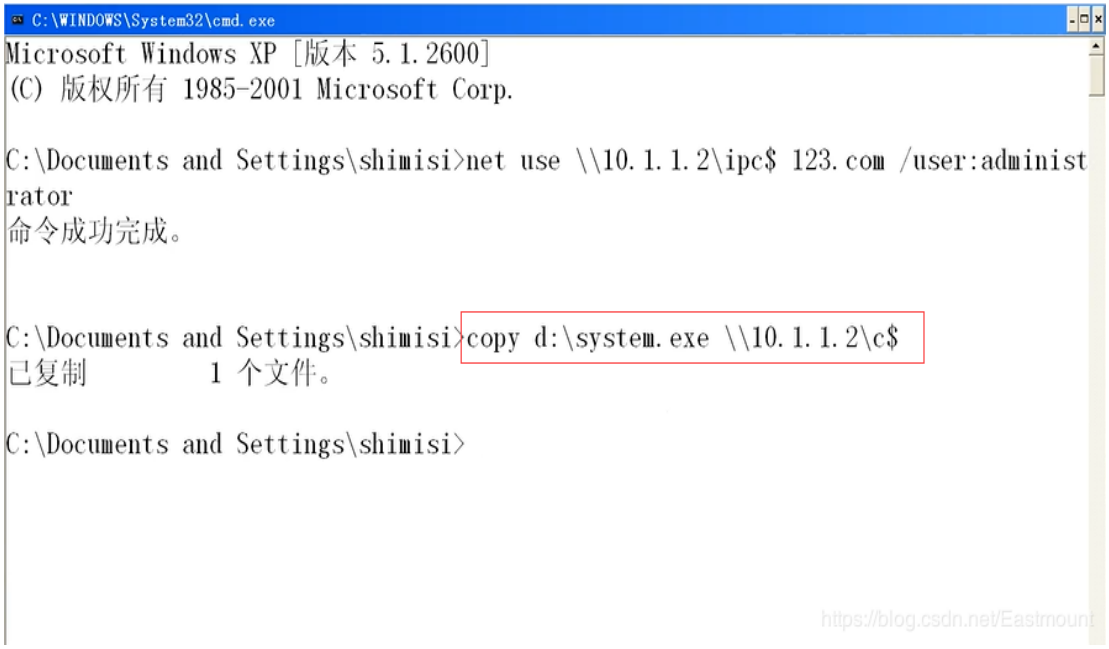


注意：一旦建立IPC $ 空连接之后，目标的 C$ 、 D$ 、E$（C盘、D盘、E盘）都不需要再输入账号和密码，可以直接进行操作。 接着我们尝试操作服务器，将木马拷贝到服务器中。怎么实现呢?

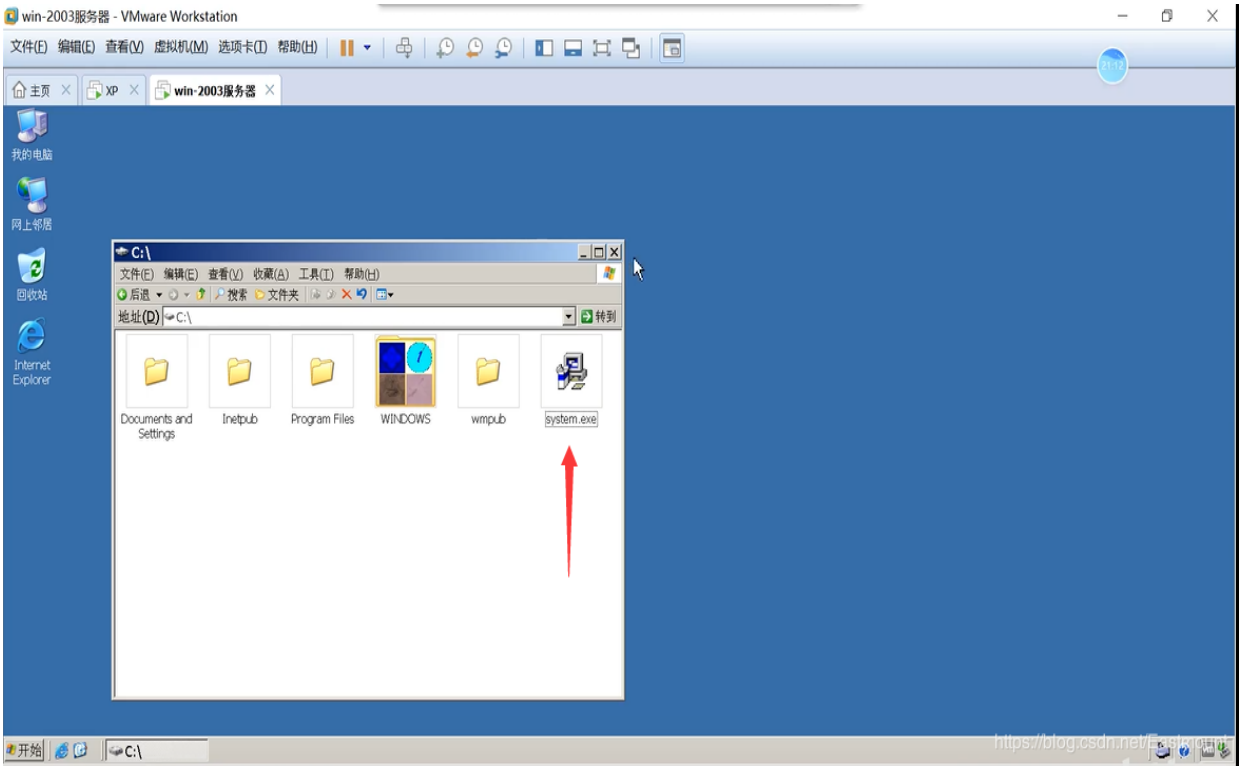
第五步，拷贝木马到服务器中。

建议大家将木马程序拷贝到C盘中深层次的目录下，这里仅拷贝到C盘根目录。

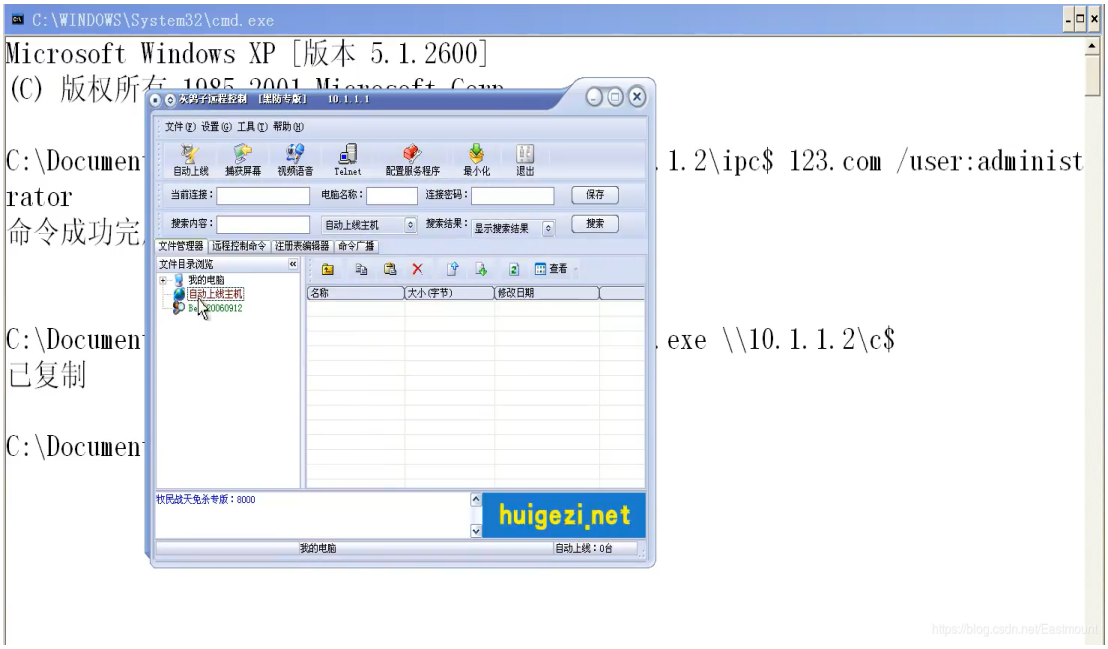
```
copy d:\system.exe \\10.1.1.2\c$
```



注意：这条copy命令之所以能够被使用，是因为我们利用445端口漏洞已经建立了空连接。此时我们查看服务器，可以看到“system.exe”程序已经被植入了。



为什么我们的HGZ软件没有提示上线呢？这是因为木马程序还没有运行。



第六步，远程运行我们的木马。

如果输入“time”是获取本机的当前时间，如果输入“net time \10.1.1.2”是获取服务器的时间。

```
C:\Documents and Settings\shimisi>time
当前时间:  9:45:11.07
输入新时间:

C:\Documents and Settings\shimisi>
C:\Documents and Settings\shimisi>net time \\10.1.1.2
\\10.1.1.2 的当前时间是 2019/6/27 上午 09:45

命令成功完成。
```


知道时间之后，我们可以通过命令给对方植入一个计划任务，计划任务可以定时执行一个程序。虽然不能双击这个程序，但是能够定时执行这个程序。

```
at \\10.1.1.2 09:50 c:\system.exe
```

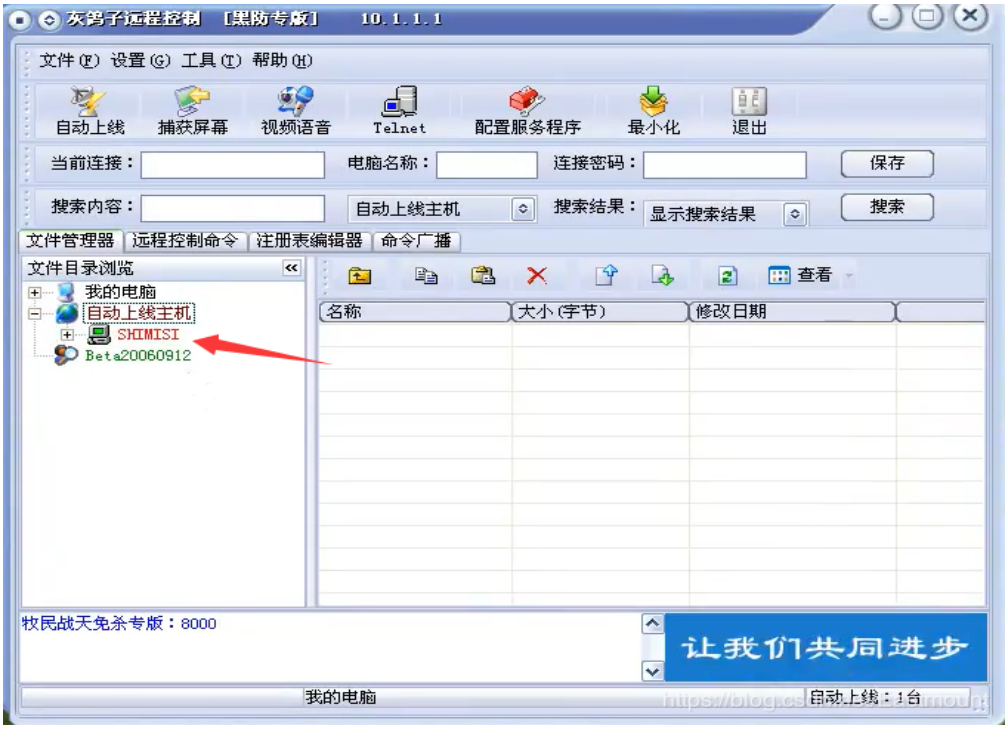
该命令表示服务器“10.1.1.2”在9点50执行system.exe程序。

```
C:\Documents and Settings\shimisi>net time \\10.1.1.2
\\10.1.1.2 的当前时间是 2019/6/27 上午 09:46

命令成功完成。


C:\Documents and Settings\shimisi>
C:\Documents and Settings\shimisi>
C:\Documents and Settings\shimisi>at \\10.1.1.2 09:50 c:\system.exe
新加了一项作业，其作业 ID = 1
```


输入命令“at \10.1.1.2”可以看到，该计划已经执行。

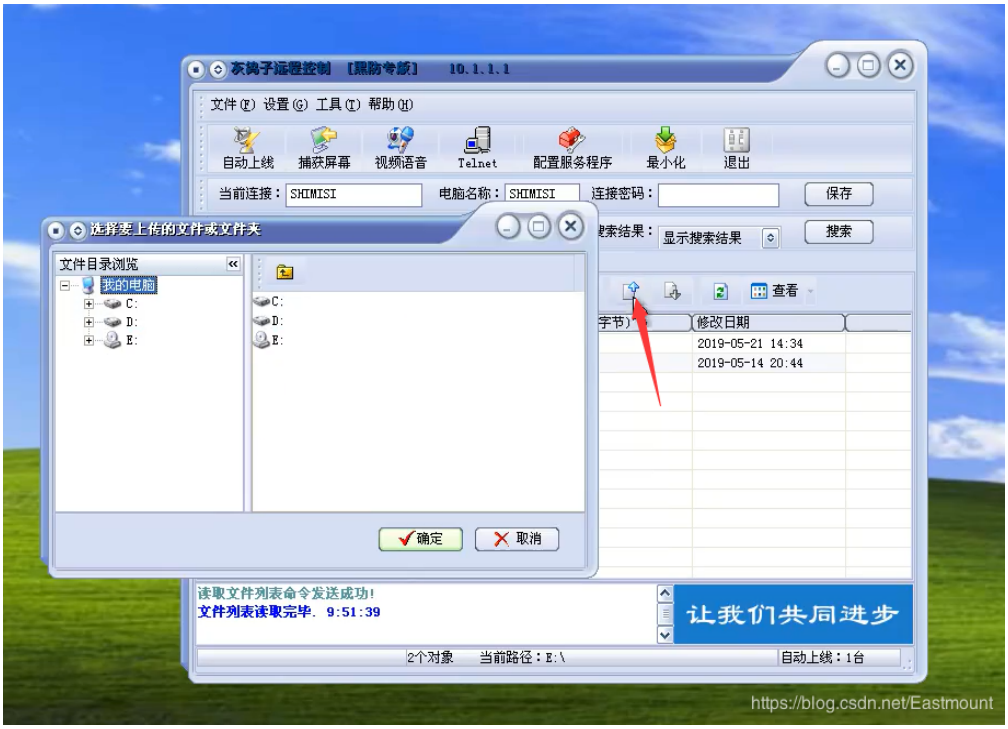
```
C:\Documents and Settings\shimisi>at \\10.1.1.2
状态 ID     日期                    时间          命令行
-------------------------------------------------------------------------------
        1   今天                    上午 09:50    c:\system.exe
```

当时间到了9点50，可以看到“SHIMISI”服务器已经上线，这就是一台被我们控制的肉鸡。

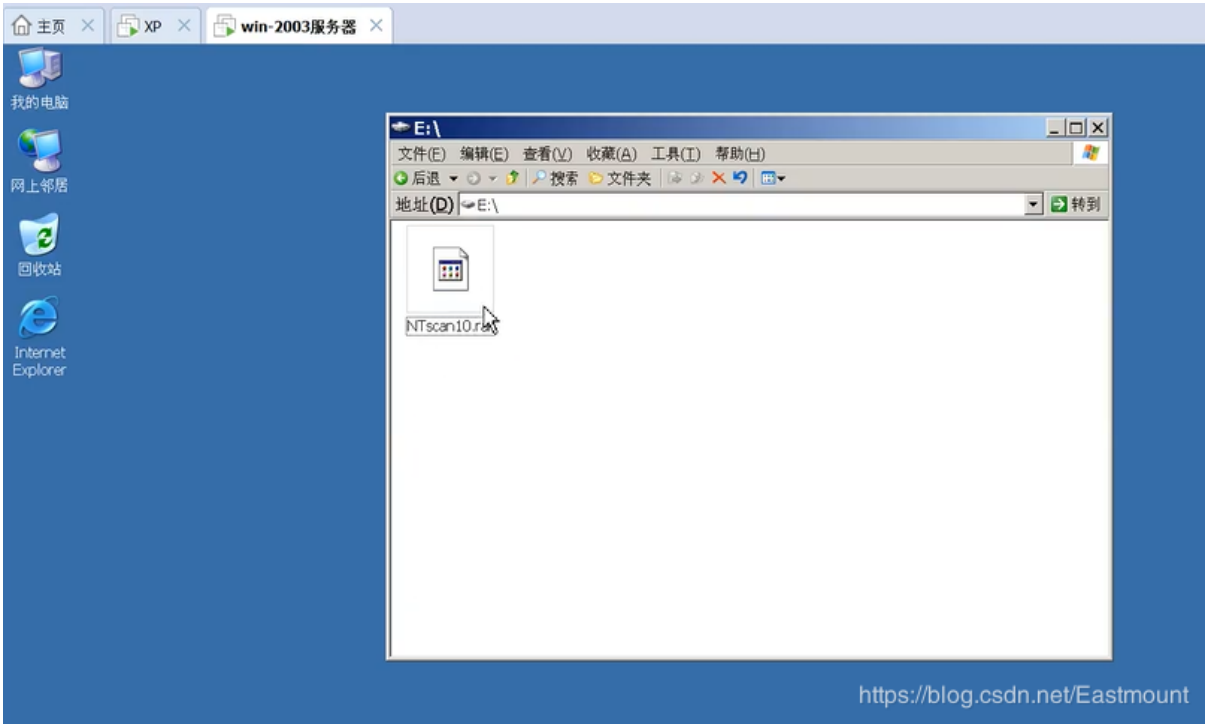


打开“SHIMISI”服务器，可以看到C盘、D盘和E盘的内容。

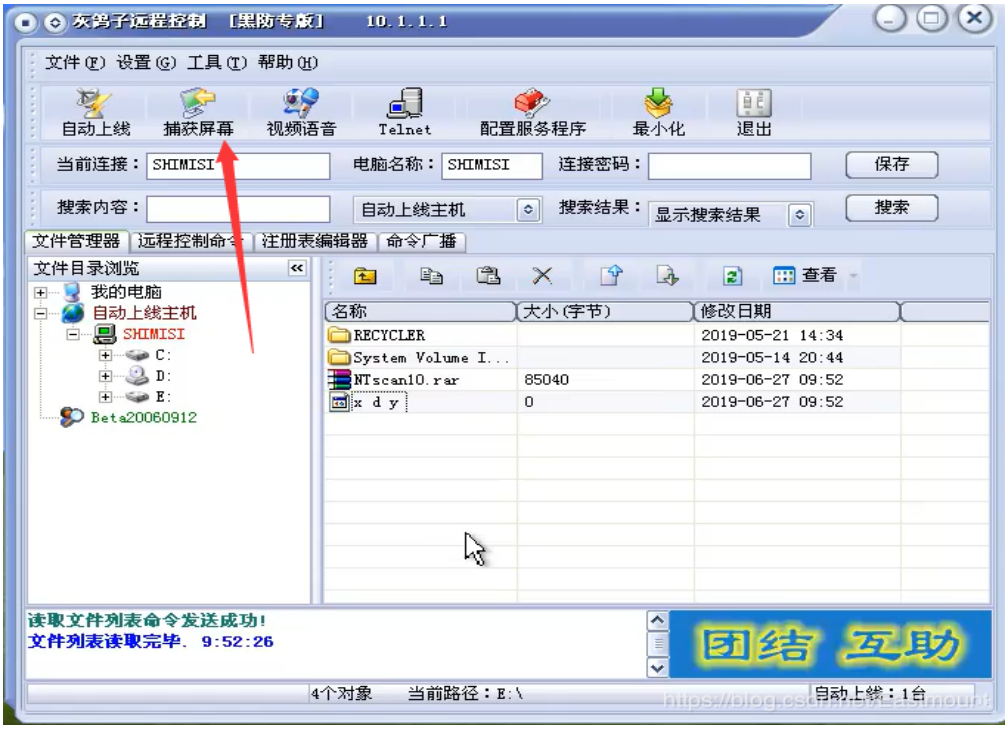
假设我们想往控制的2003服务器传文件，选中E盘，然后点击上传图标，选择本地软件后点击“确定”。



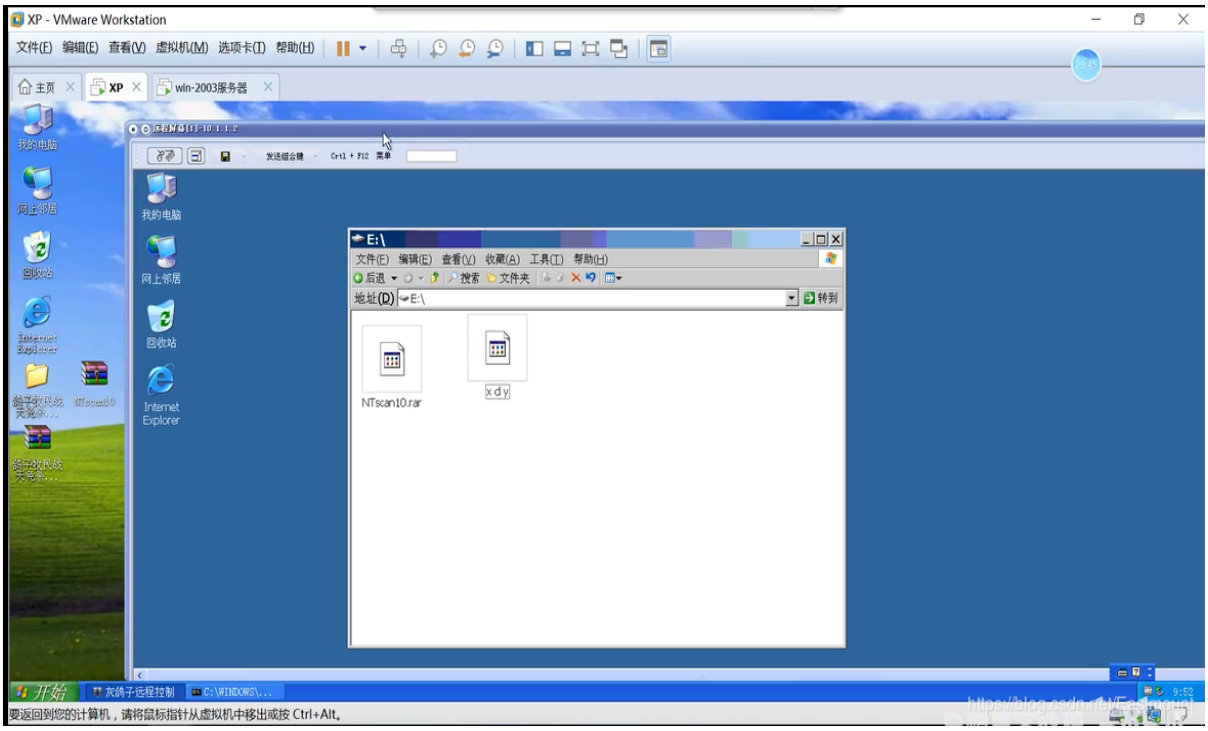
可以看到，对方电脑E盘中出现了我们上传的文件。同样，我们可以将对方服务器的内容下载至本地。



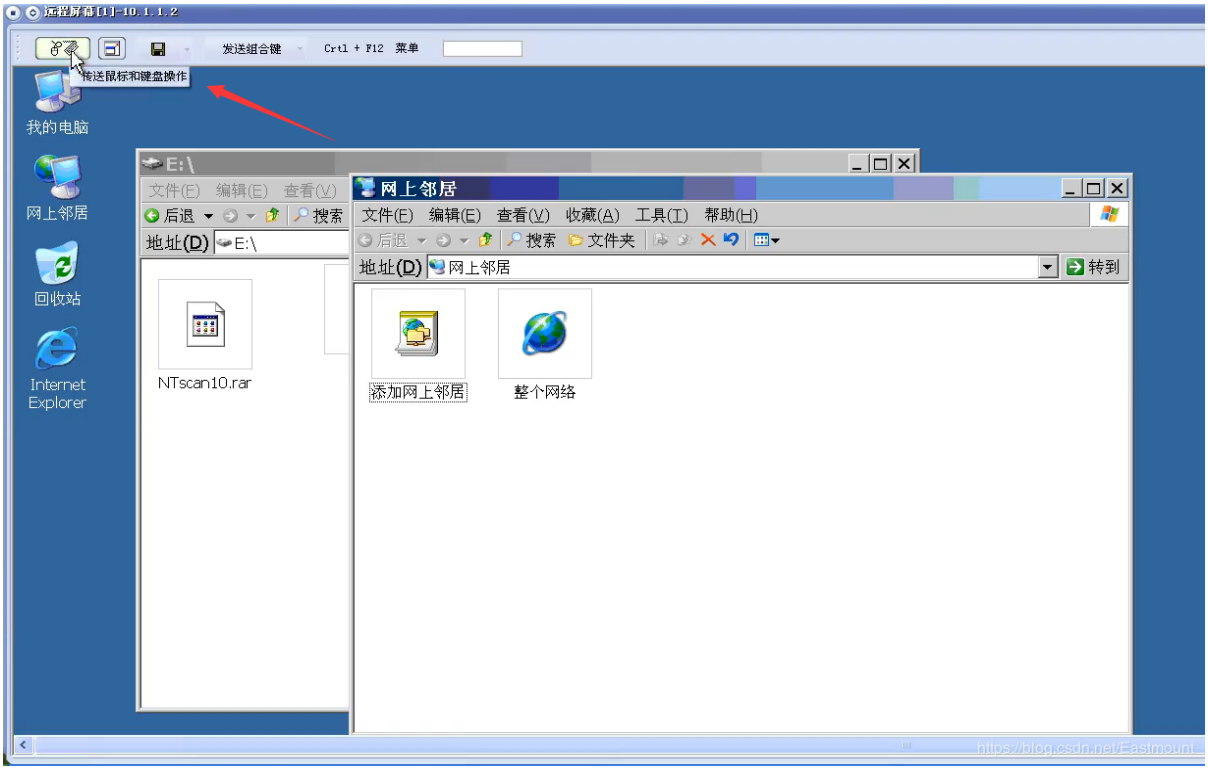
点击“捕获屏幕”按钮。



可以看到对方的屏幕已经被成功控制，而且为实时画面。

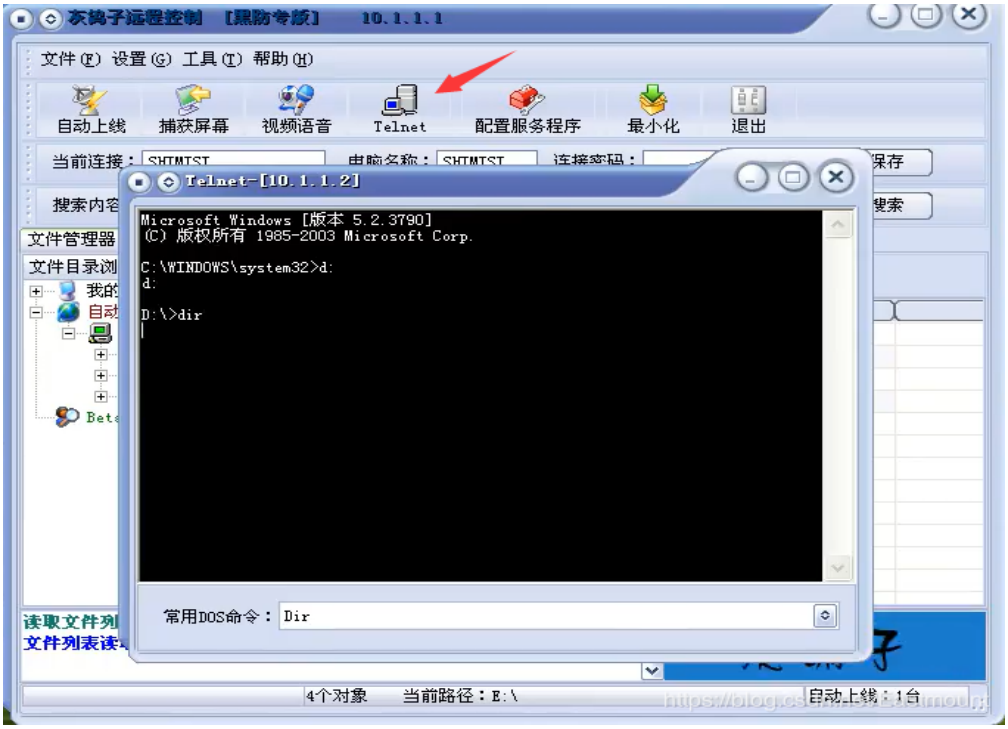


点击左上角“传送鼠标和键盘操作”，可以接管控制服务器电脑的鼠标和键盘。



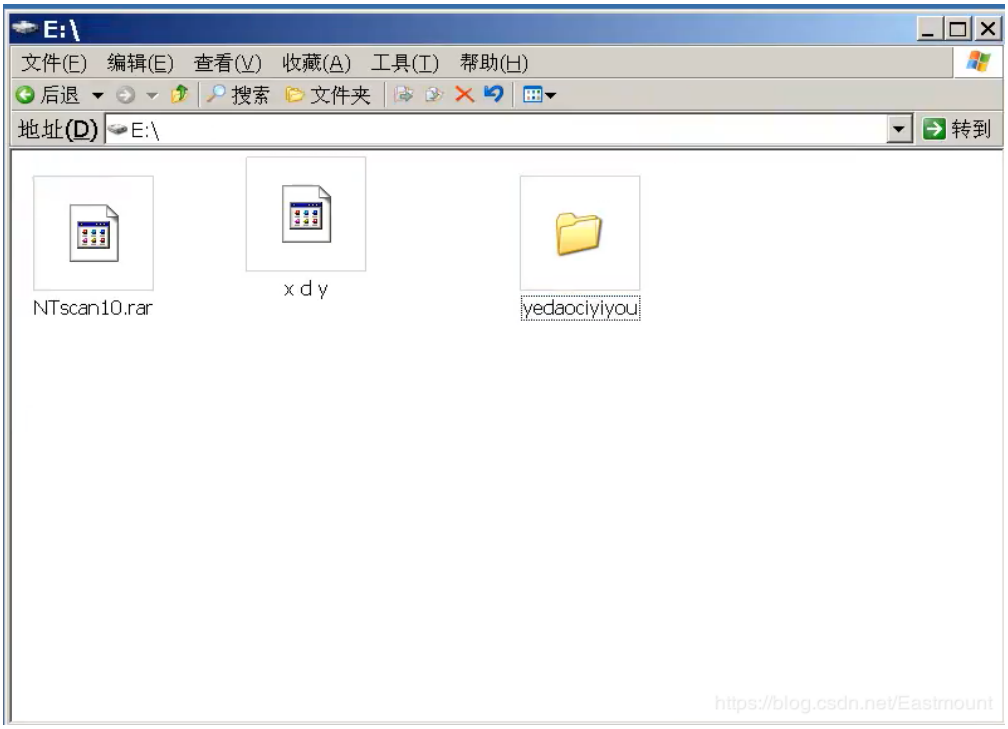
点击“视频语音”按钮，再点击“开始视频监控”，可以进行摄像头拍摄。所以大家一定注意，平时不用要关闭摄像头或封住。

点击“Telnet”图标可以进行命令行控制。

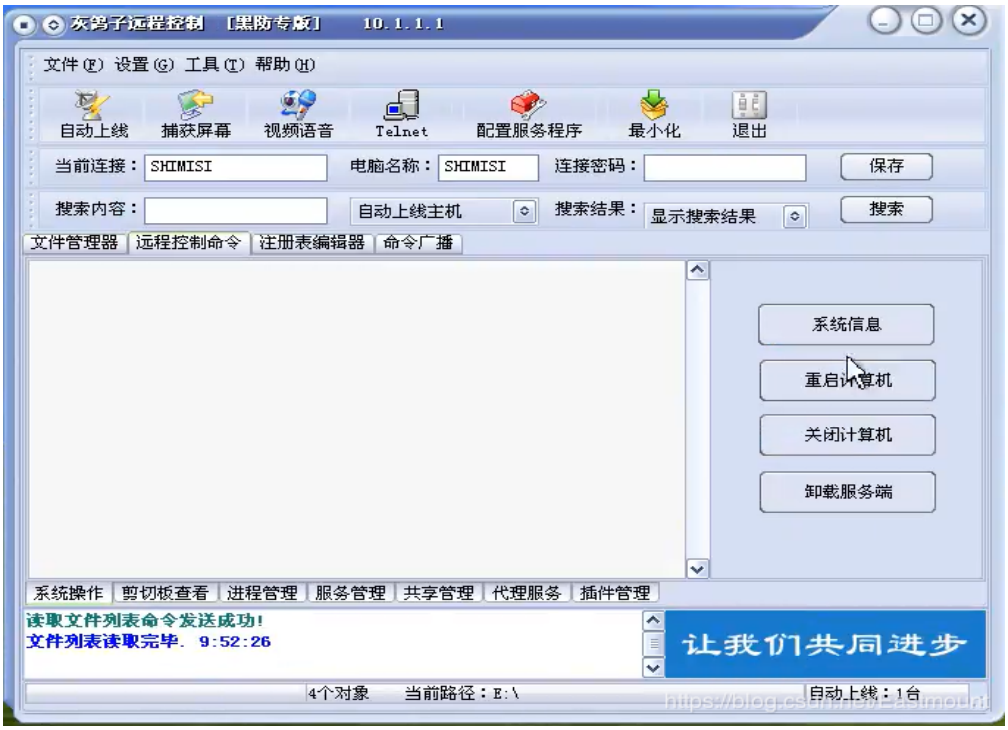


比如在E盘调用命令“md yedaociyiyou”，可以创建文件夹。

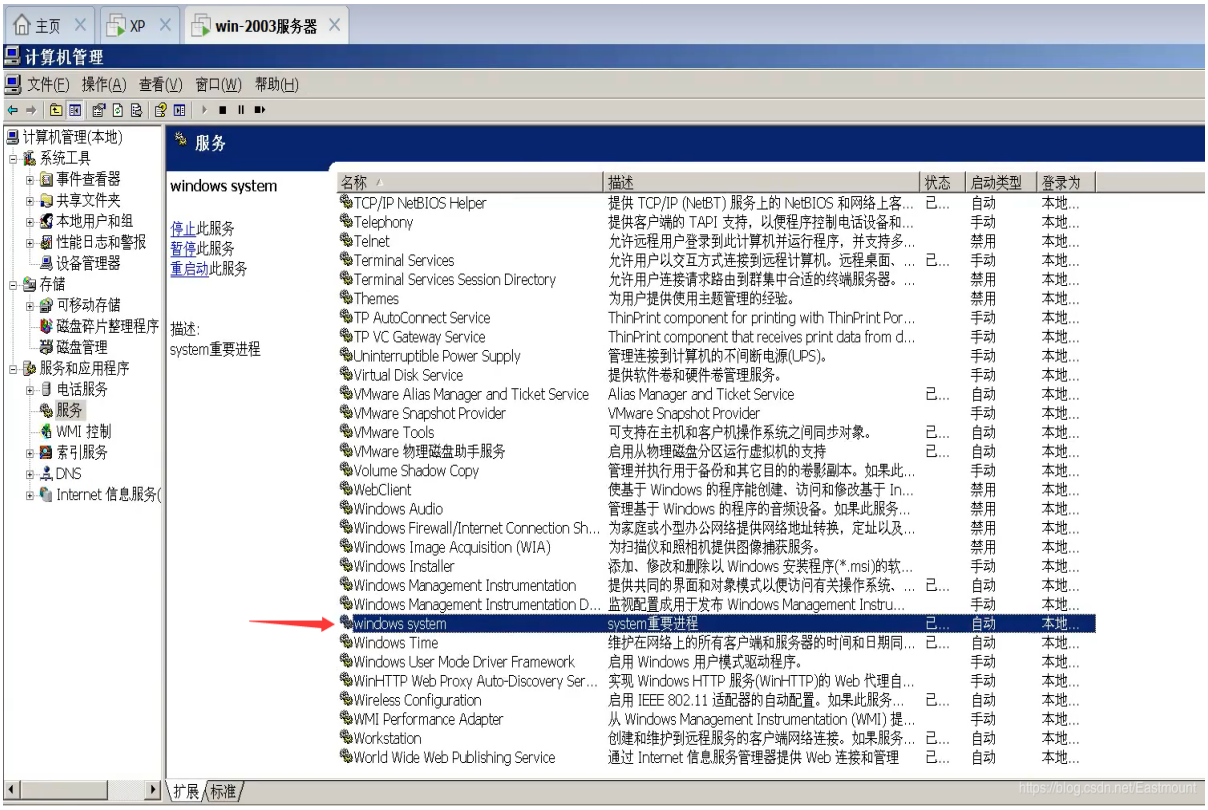
服务器成功创建了该文件夹。



远程控制命令比如关机重启等，注册表修改等。



注意：该木马修改了服务，只要开机就会自动运行该木马而为我们所用。

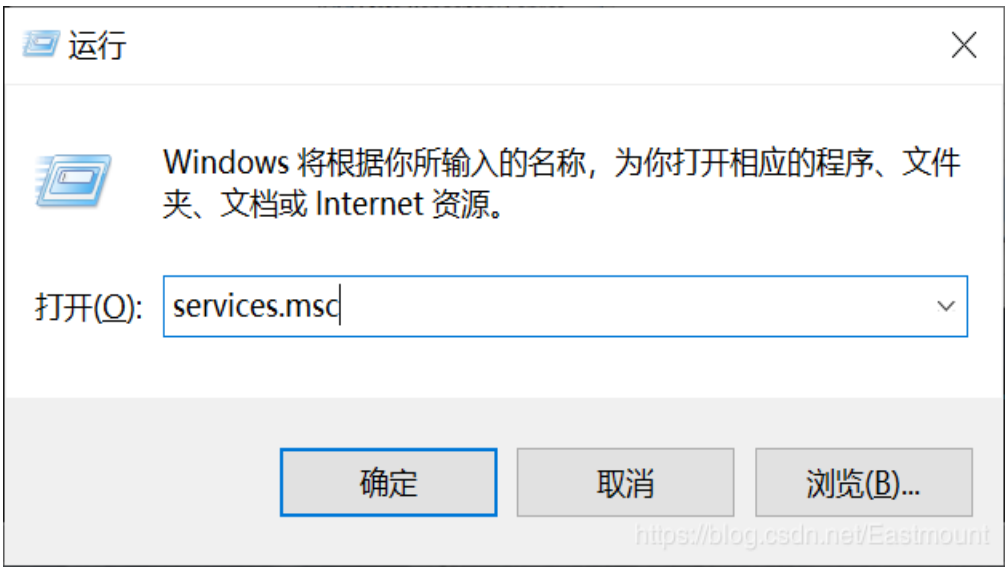


> 再次声明：HGZ木马现在很容易被杀死或察觉，也有不容易被杀死，大家一定不能拿去用于攻击，它会违反相关的法律，HGZ的作者可能还在里面。我们作为安全工程师，希望您们去了解漏洞背后的原理，更好地进行防御，绿色网络需要我们共同维护。

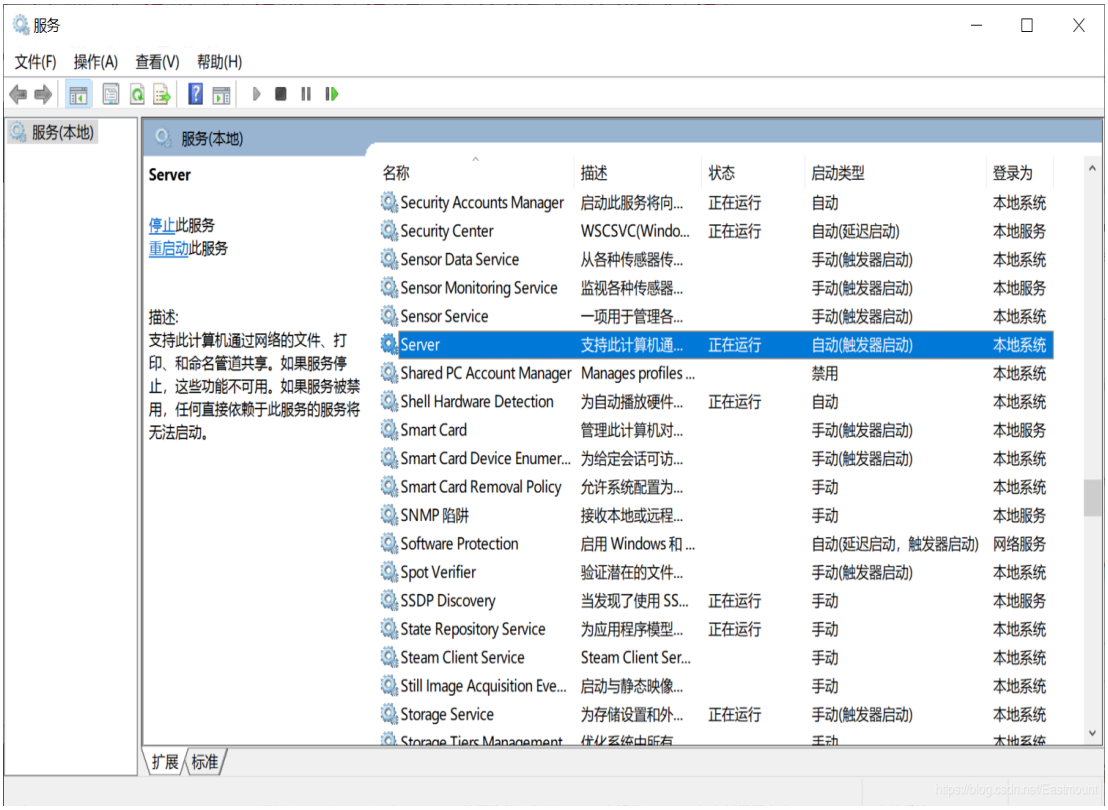
补充：如何关闭远程服务或445端口呢？

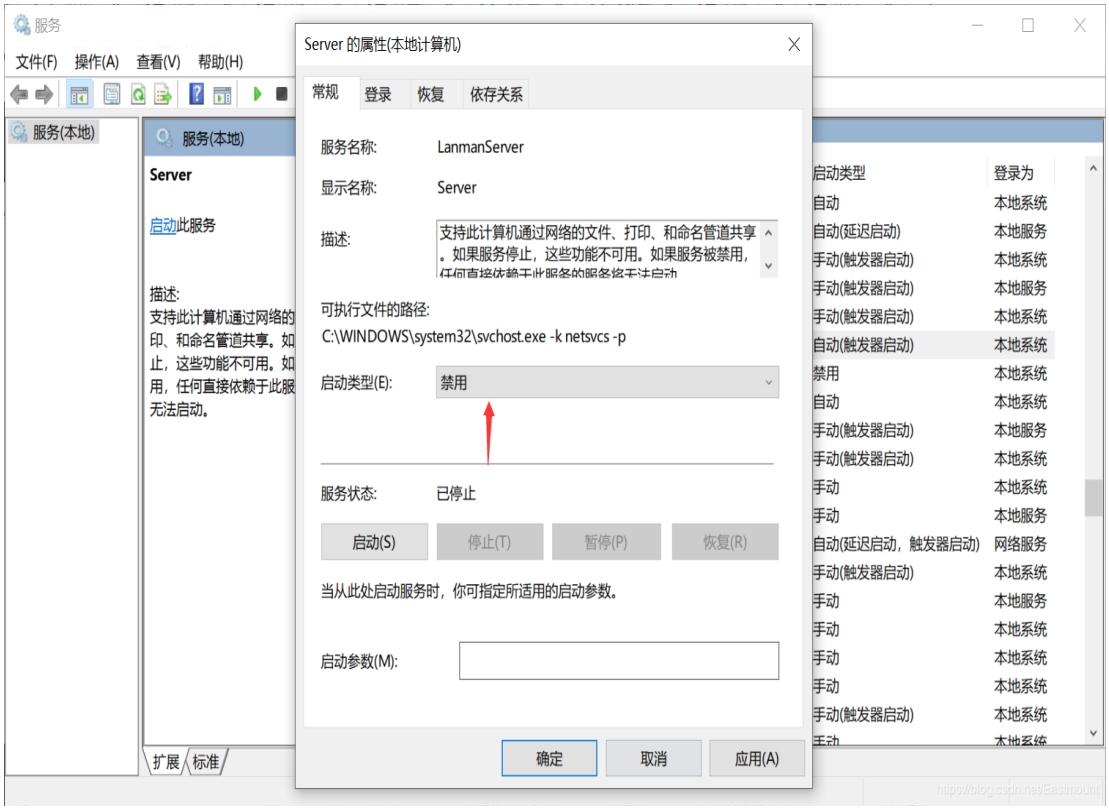
作者打开自己的笔记本，输入命令“net share”，可以看到共享服务都是启动的，这是存在漏洞的。

在运行中输入services.msc，然后找到服务。

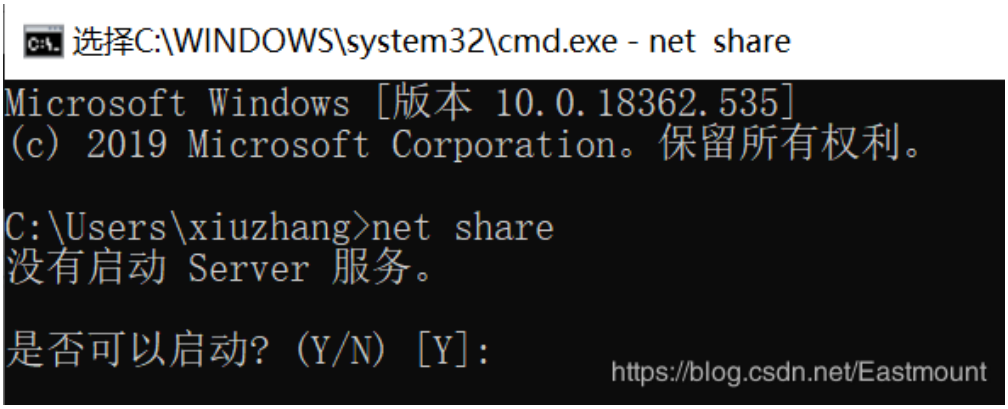


我们需要将它关闭，设置为“禁用”。

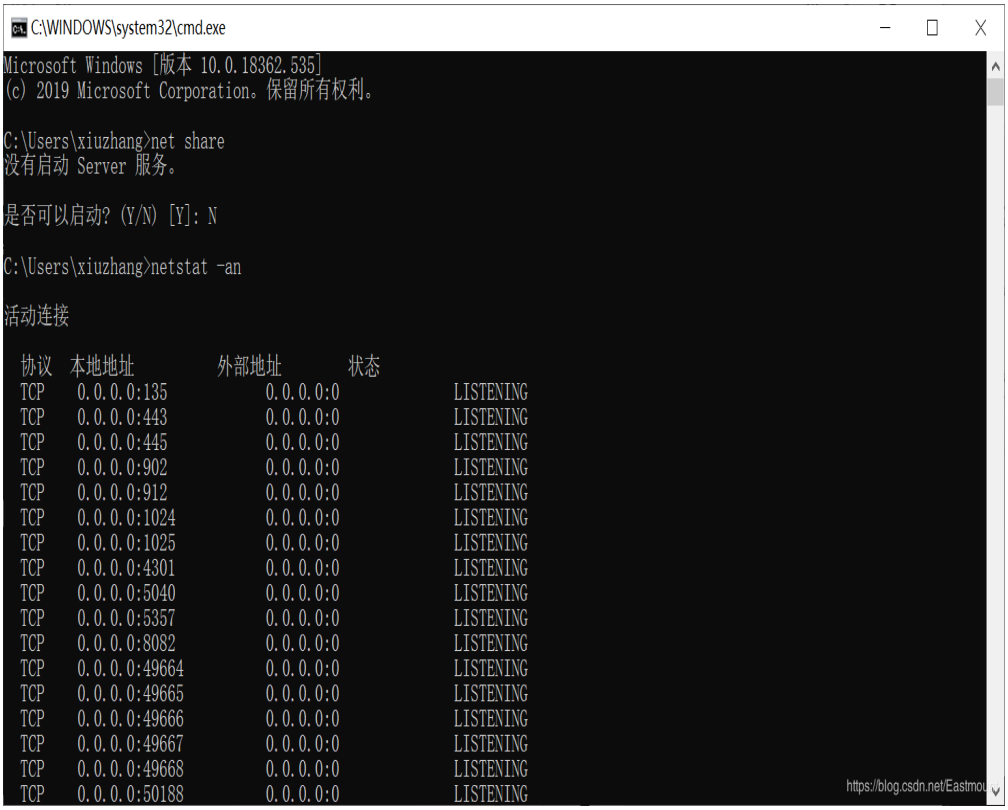




再次运行，发现共享服务被成功关闭。



netstat -an命令能看到所有和本地计算机建立连接的IP，它包含四个部分：proto（连接方式）、local address（本地连接地址）、foreign address（和本地建立连接的地址）、state（当前端口状态）。通过这个命令的详细信息可以完全监控自己的计算机上的连接。



三.总结

写到这里，这篇基础性文章就此结束。本文详细讲解了木马的原理知识，通过远程服务器445端口相关的IPC $ 漏洞复现了一个木马制作、植入、运行、控制的过程，作者的初衷一方面是做网络安全的普及，另一方面希望提高读者的安全防范意识。如何防御呢?

- 提高警惕性，别占小便宜，别点击垃圾链接或邮件
- 从官网下载程序，密码设置复杂，防止弱口令（数字大小写符号）爆破
- 设置防火墙和杀毒软件，定期杀毒并清理电脑
- 防止社会工程学诱骗或攻击
- 关于软件或系统漏洞，及时关闭远程服务或端口
- 摄像头、麦克风、路由器、网关、服务器等系统漏洞及人为防御
- 禁止禁止禁止做任何危害网络安全的行为，作为安全工程师，需要我们共同维护绿色网络

希望这系列文章对您有所帮助，真的感觉自己技术好菜，要学的知识好多。这是第43篇原创的安全系列文章，从网络安全到系统安全，从木马病毒到后门劫持，从恶意代码到溯源分析，从渗透工具到二进制工具，还有Python安全、顶会论文、黑客比赛和漏洞分享。未知攻焉知防，人生漫漫其路远兮，作为初学者，自己真是爬着前行，感谢很多人的帮助，继续爬着，继续加油。

侠之为大，为国为民。向一线医护人员、军人、工人、科学家和所有工作者致敬。咱们中国人一生的最高追求，为天地立心，为生民立命，为往圣继绝学，为万世开太平，他们真的做到了。生活哪有什么岁月静好，只不过这些人替我们负重前行。希望每一个人都健康平安，戴口罩不出门，勤洗手多吃饭。武汉加油，湖北加油，中国加油。众志成城，加油必胜！！！

> 最后希望大家帮我CSDN博客之星投投票，每天可以投5票喔，谢谢大家！八年，在CSDN分享了410篇文章，65个专栏，400多万人次浏览，包括Python人工智能、数据挖掘、网络爬虫、图象处理、网络安全、JAVA网站、Android开发、LAMP/WAMP、C#网络编程、C++游戏、算法和数据结构、面试总结、人生感悟等。当然还有我和你的故事，感恩一路有你，感谢一路同行，希望通过编程分享帮助到更多人，也希望学成之后教更多学生。因为喜欢，所以分享，且看且珍惜，加油！我的学生们，等我学成归来～
>
> 投票地址：http://m234140.nofollow.ax.mvote.cn/opage/ed8141a0-ed19-774b-6b0d-39c3aaf89dde.html?from=singlemessage

(By:Eastmount 2020-01-30 深夜9点写于贵阳 http://blog.csdn.net/eastmount/)

参考文献：

[1] 2019 黑客入门基础Windows网络安全精讲 - B站老师