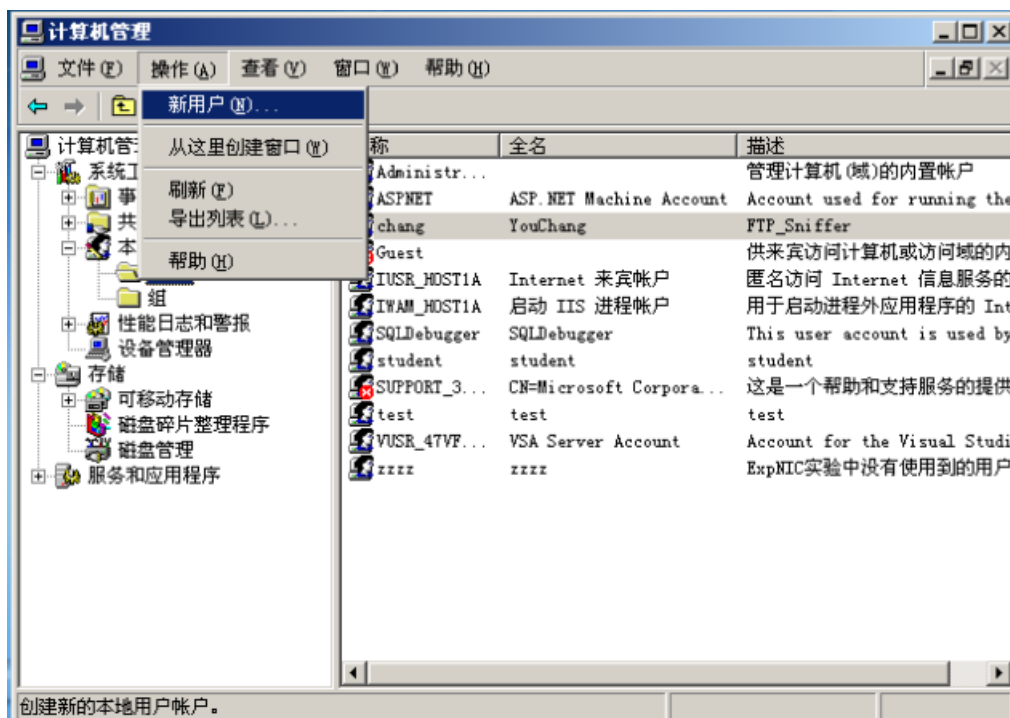


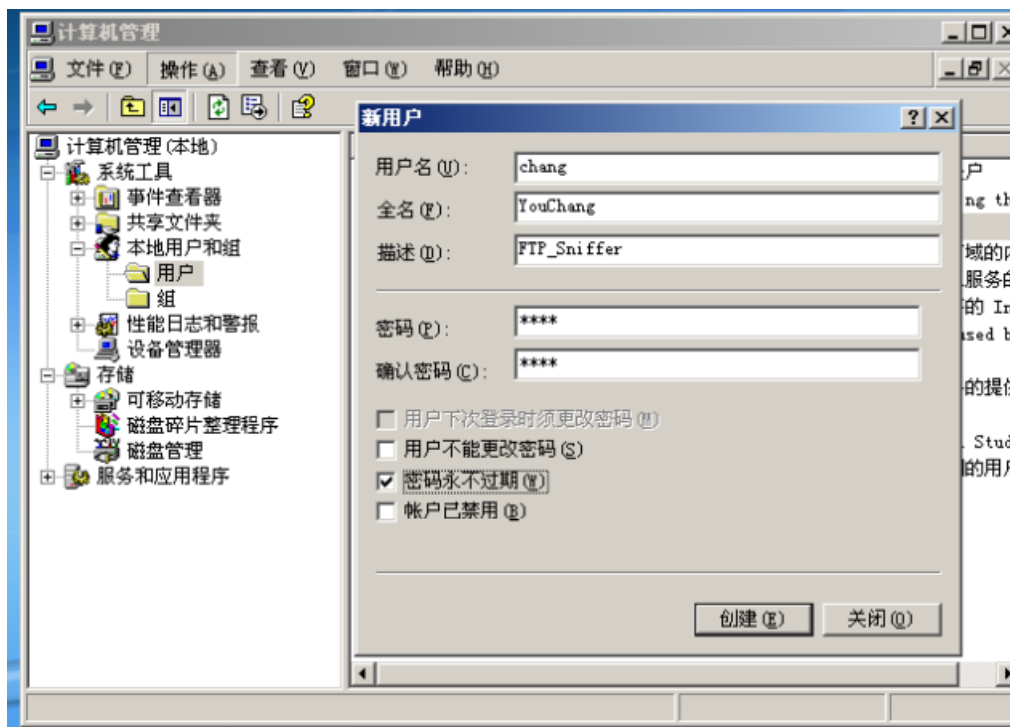


《网络与信息安全》课程实验报告

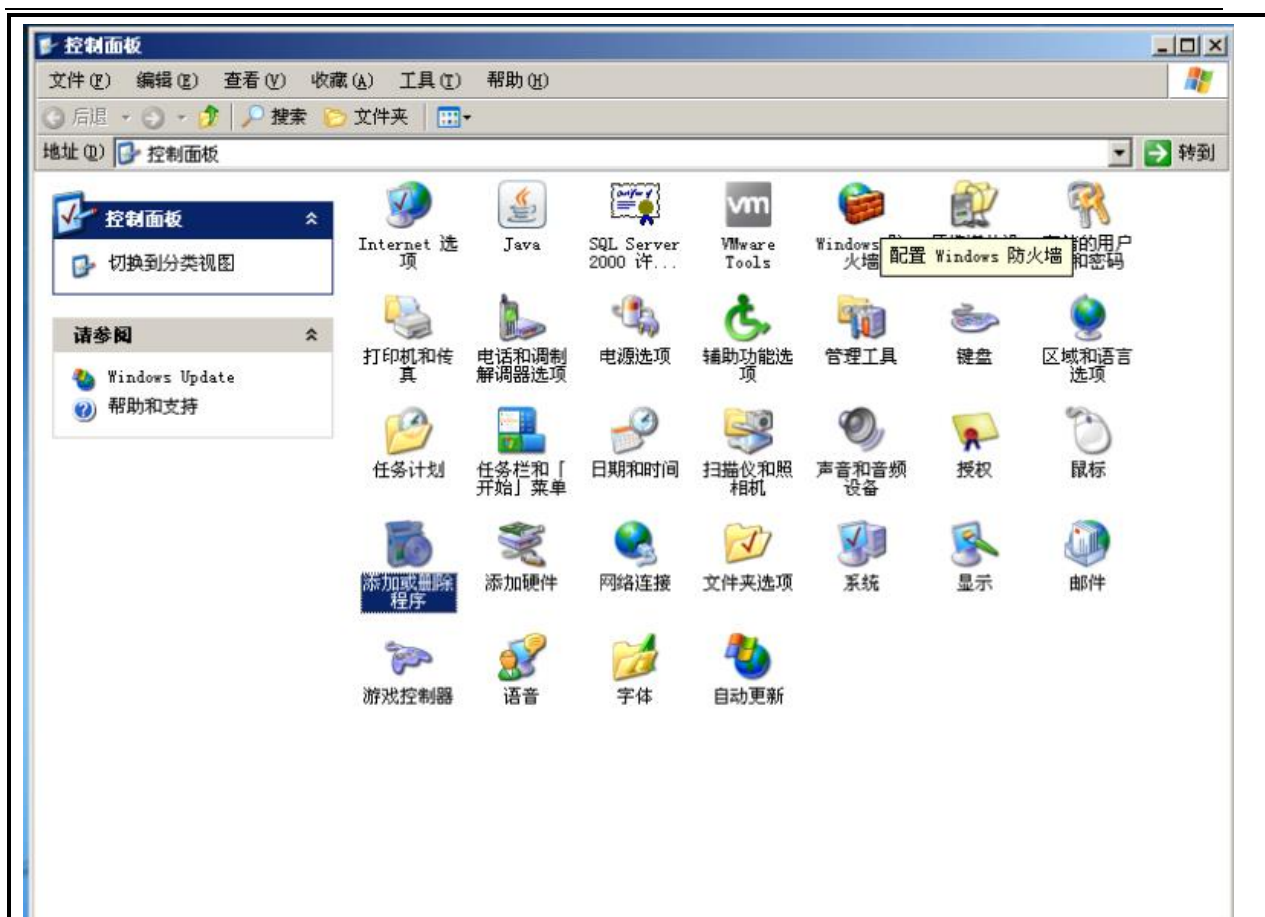
实验名称	FTP 嗅探		
实验人员	游畅	学 号	20181003005
实验日期	2021. 04. 21		
<p>一、 实验目的</p> <ol style="list-style-type: none">1、 熟悉 FTP 协议的工作原理与传输方式；2、 了解 FTP 协议的指令以及代码；3、 通过实验嗅探得到明文账号及密码，从而加强网络安全意识。			
<p>二、 实验环境</p> <ol style="list-style-type: none">1、 Vmware in Windows 72、 Windows Server 20033、 中软吉大网络安全实验平台			
<p>三、 实验原理</p> <p>本次实验包括了以下两块内容，分别是：1)、FTP 站点架设；2)、使用中软吉大的平台的协议分析器进行抓包解析。</p> <ol style="list-style-type: none">1、 服务器架设使用 windows 系统自带的 IIS (互联网信息服务) 完成，步骤见下；2、 协议分析器的原理是通过网络接口截取数据报文，然后加以分析			
<p>四、实验步骤</p> <ol style="list-style-type: none">1、首先在系统内新建用户，分配用户名以及密码；*账号：chang；密码：1928*。2、利用 IIS 架设 FTP 站点，并选择文件夹路径；*设置文件夹名字即为 FTP_Sniffer，文本文件“hello.txt”*3、打开协议分析器，准备进行抓包；4、从另一台机器远程访问本机的 FTP 文件夹；5、回到本机查看抓包结果，并予以记录分析。			
<p>五、实验记录</p> <ol style="list-style-type: none">1、打开计算机管理页面，新建用户			



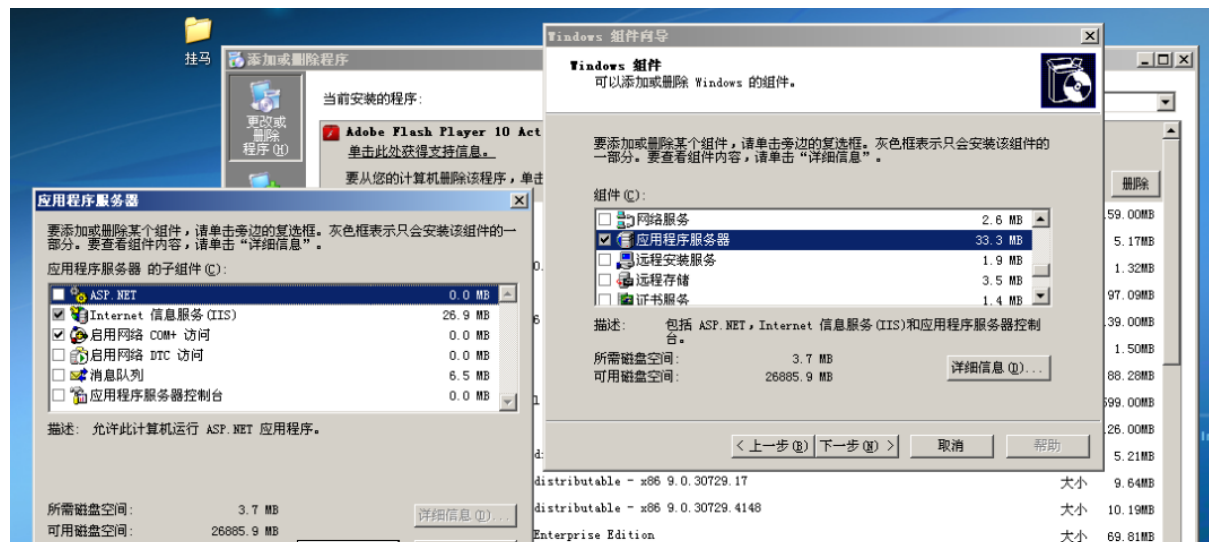
2、设置用户名密码



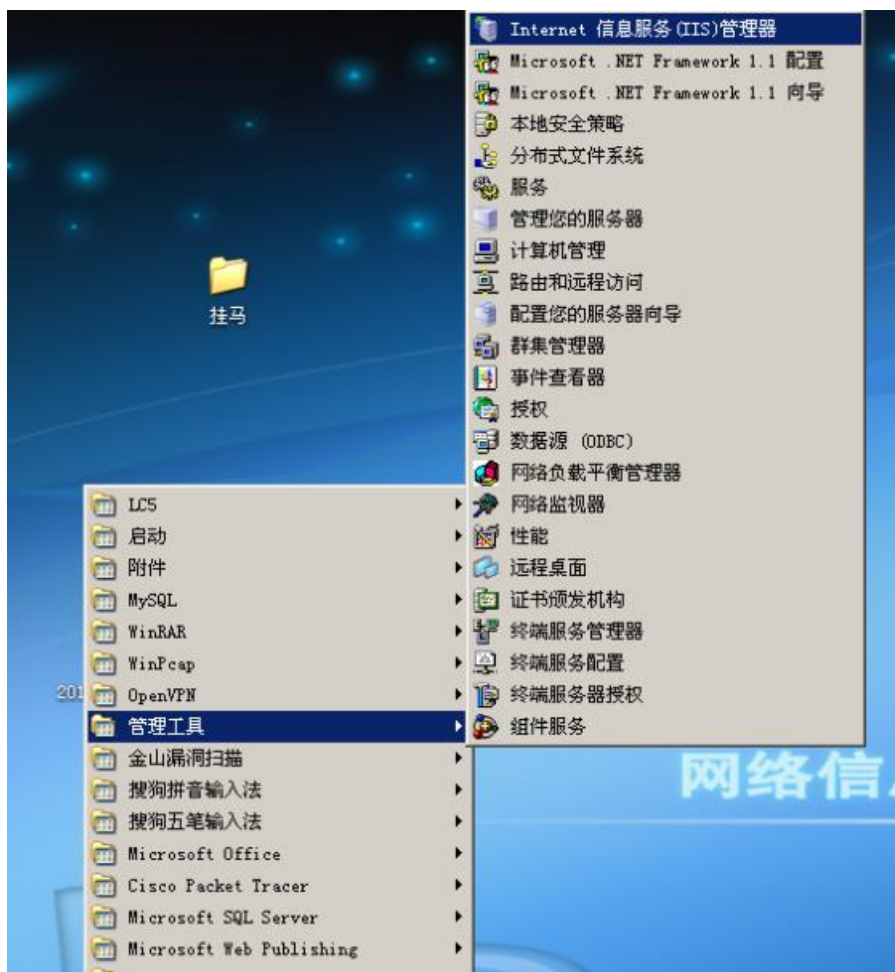
3、打开控制面板，单击“添加或删除程序”开启 IIS 服务；



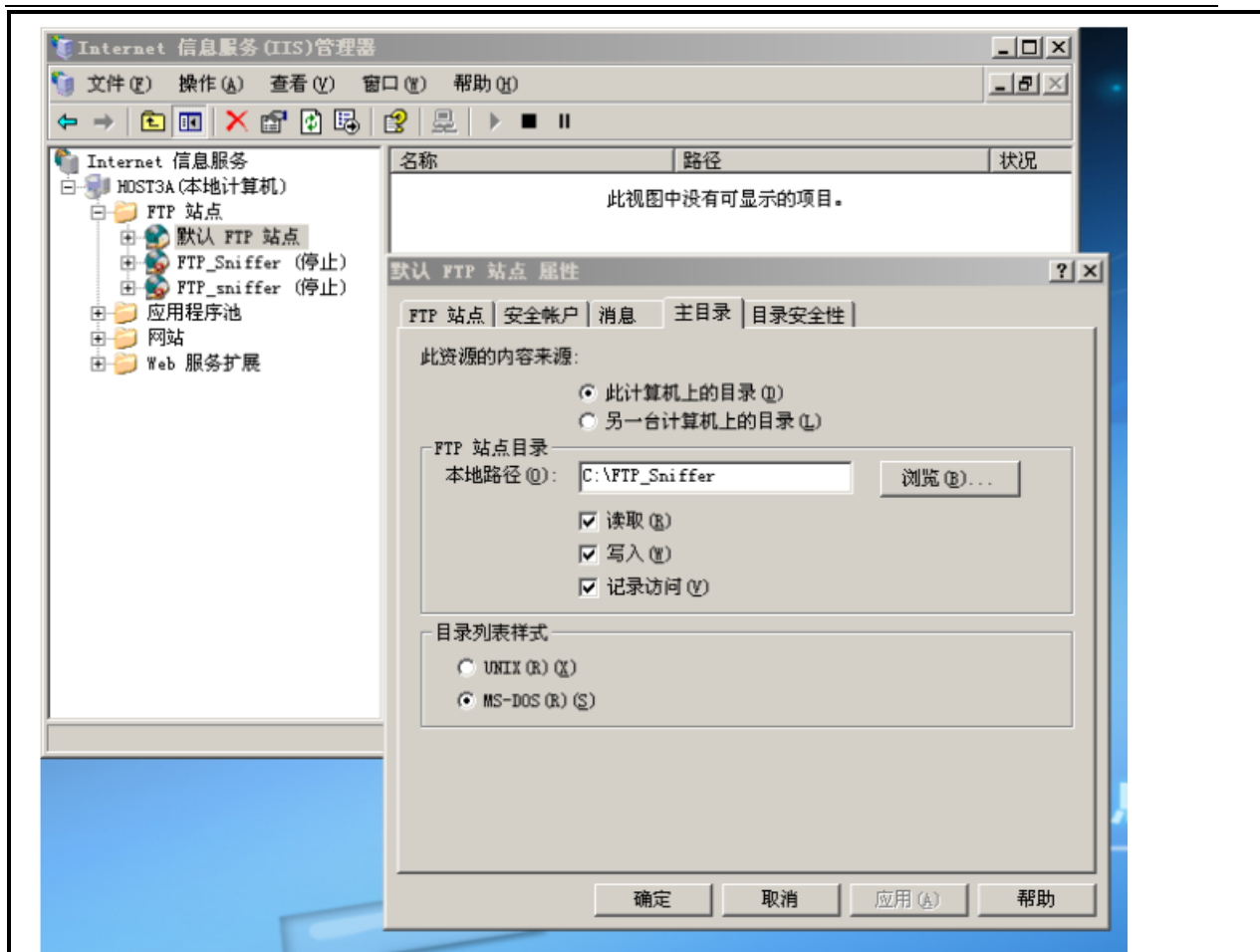
4、依次单击 组件向导-应用程序服务器，勾选 IIS 服务，等待安装完成。



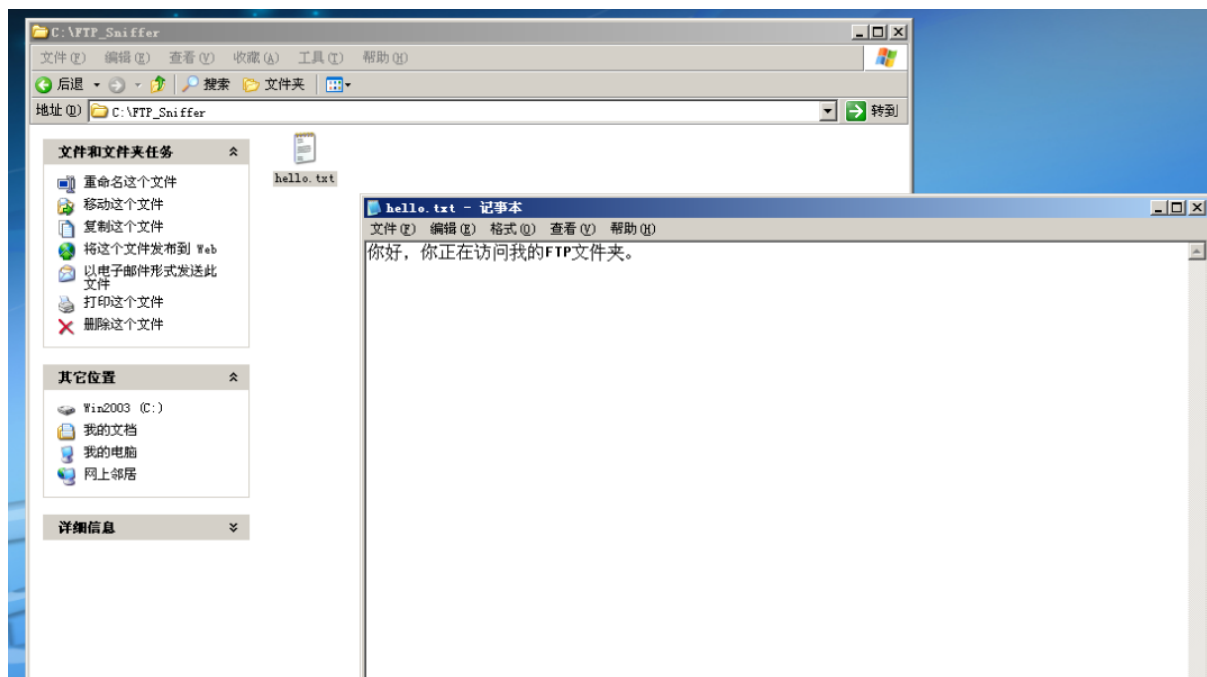
5、安装完成后，进入 管理工具 -> IIS 管理器。



6、右键默认 FTP 站点，选中属性进行本地路径配置（路径为 “C:\FTP_Sniffer”）



7、在该目录下新建记事本以及 hello.txt



8、查看本机 ip 地址，为 172.16.0.31，网关 172.16.0.253



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

D:\ExpNIC>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.0.31
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 172.16.0.253

D:\ExpNIC>
```

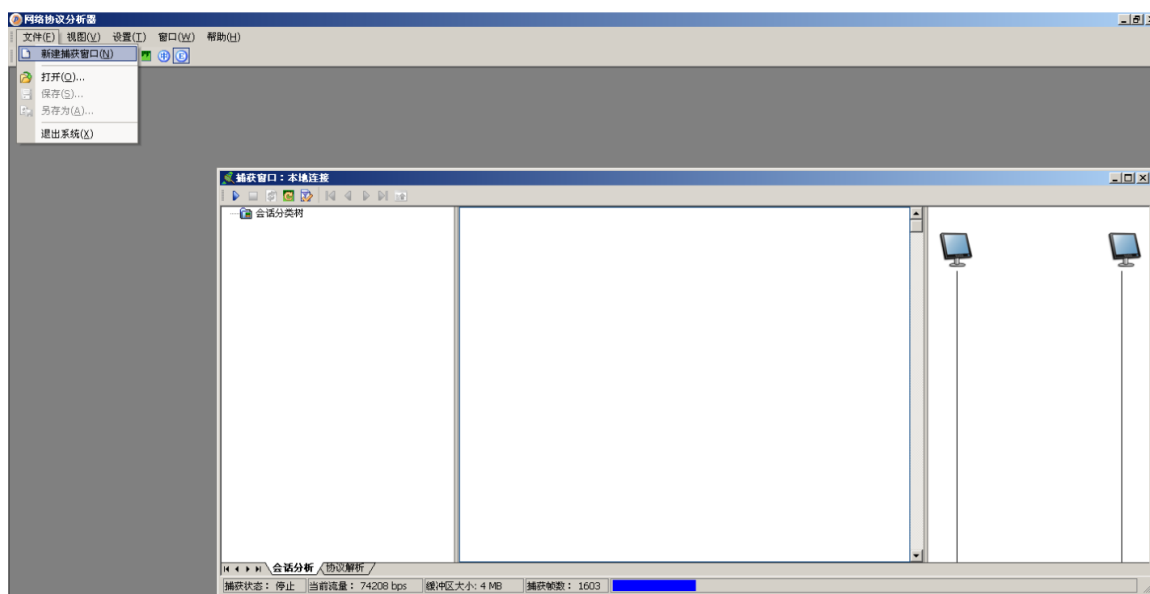
9、尝试本地访问 FTP 服务器，成功

```
C:\WINDOWS\system32\cmd.exe - ftp 172.16.0.31

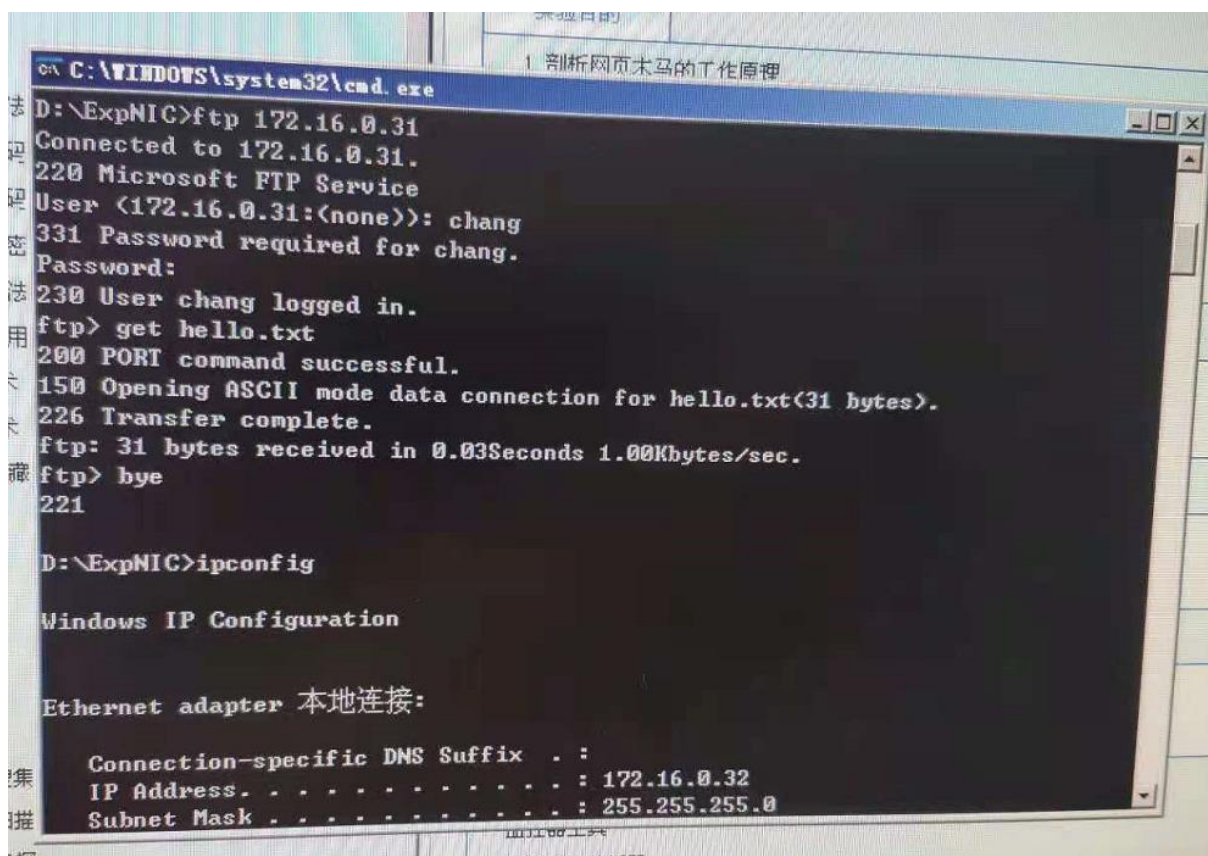
Connection-specific DNS Suffix  . : 
IP Address. . . . .               : 172.16.0.31
Subnet Mask . . . . .             : 255.255.255.0
Default Gateway . . . . .         : 172.16.0.253

D:\ExpNIC>ftp 172.16.0.31
Connected to 172.16.0.31.
220 Microsoft FTP Service
User (172.16.0.31:(none)): chang
331 Password required for chang.
Password:
230 User chang logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
hello.txt
226 Transfer complete.
ftp: 11 bytes received in 0.00Seconds 11000.00Kbytes/sec.
ftp> hello.txt
Invalid command.
ftp> get hello.txt
200 PORT command successful.
150 Opening ASCII mode data connection for hello.txt(31 bytes).
226 Transfer complete.
ftp: 31 bytes received in 0.02Seconds 1.94Kbytes/sec.
ftp>
```

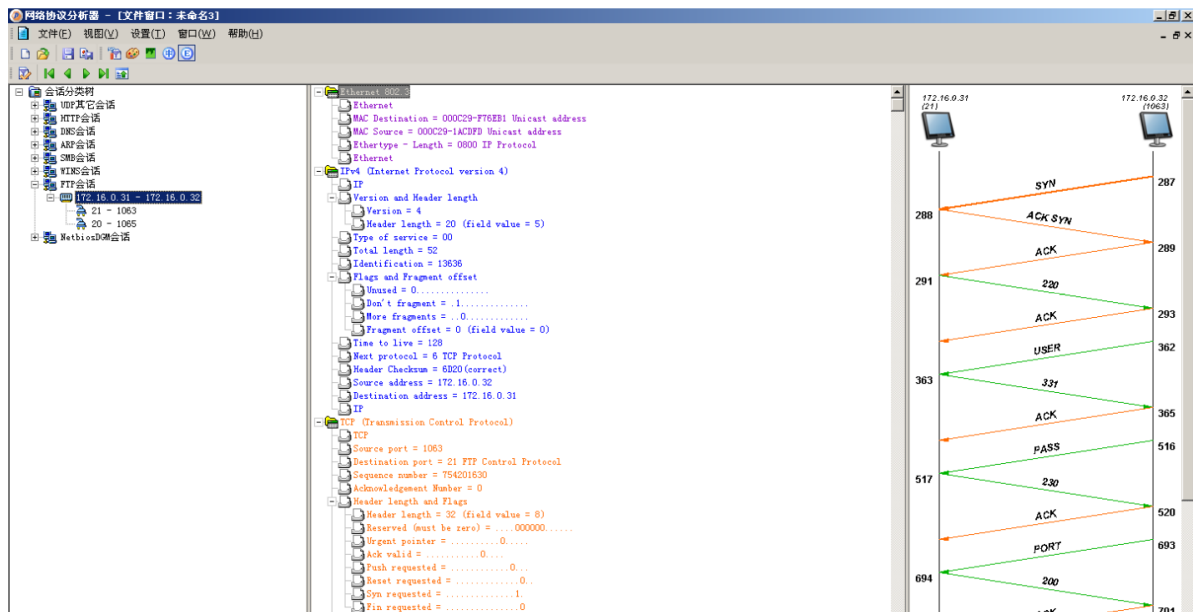
10、开启协议分析器



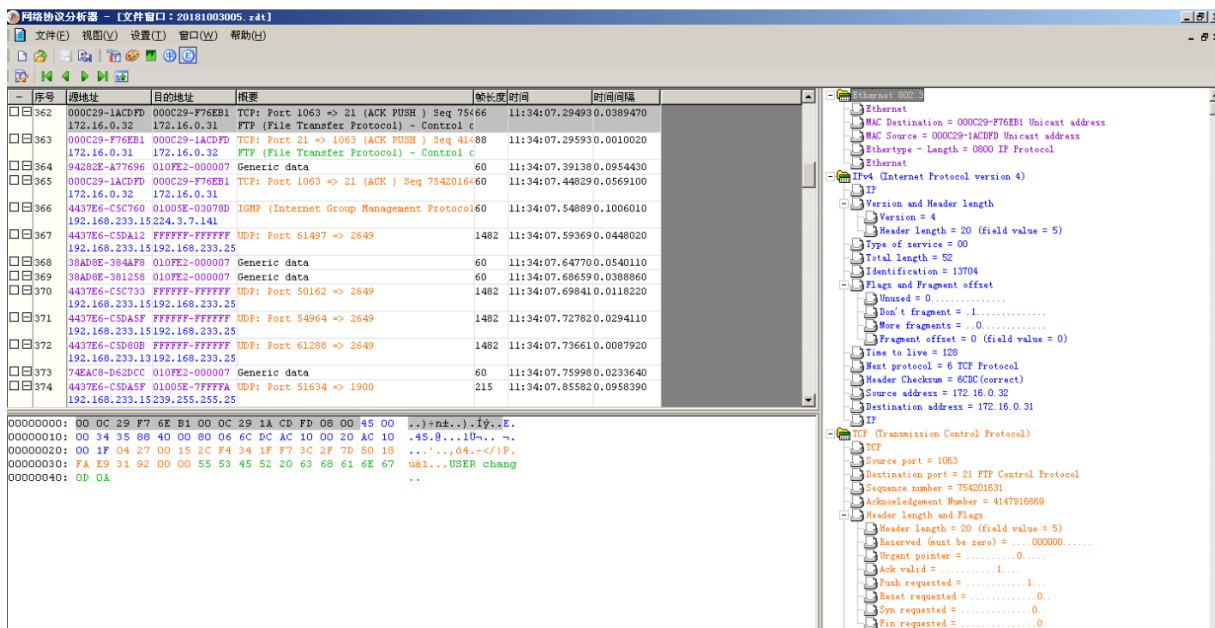
11、启动后使用另一台终端，首先查看 ip 地址（172.16.0.32），并且远程访问 FTP 文件夹：



12、访问成功后，查看协议分析器 -> 会话分类树，选择 FTP 会话，并筛选本地机与远程机的 ip;



13、选择三次握手后的“USER”线段，查看用户名：



14、同样地，选择“PASS”段查看密码：



网络协议分析器 - [文件窗口: 20181003005.rdt]

文件(F) 视图(V) 设置(I) 窗口(W) 帮助(H)

15、查看下载的文件内容:

六、实验结果分析

我们可以看出, FTP 默认使用的传输方式是明文传输, 甚至包括用于鉴权的用户名以及密码, 这使得安全性大大降低。

因此为了保证数据安全, 我们有必要加设例如 SSL 之类的功能来提高服务器数据传输的安全性。

序号	源地址	目的地址	概要	帧长度	时间	时间间隔
516	000C29-1ACDFD	000C29-F76EB1	TCP: Port 1063 => 21 (ACK PUSH) Seq 75465	11:34:12.472540	0.0065280	
517	172.16.0.32	172.16.0.31	FTP (File Transfer Protocol) - Control c	11:34:12.474000	0.0014540	
518	000C29-F76EB1	000C29-1ACDFD	TCP: Port 21 => 1063 (ACK PUSH) Seq 41481	11:34:12.474000	0.0014540	
519	172.16.0.31	172.16.0.32	FTP (File Transfer Protocol) - Control c	11:34:12.482560	0.0085650	
520	4437E6-C5C753	01003E-03078D	IGMP (Internet Group Management Protocol) 60	11:34:12.559570	0.0770040	
521	192.168.233.15	192.168.233.25	UDP: Port 1024 => 1900	11:34:12.589180	0.0296130	
522	000C29-1ACDFD	000C29-F76EB1	TCP: Port 1063 => 21 (ACK) Seq 7542016560	11:34:12.589180	0.0296130	
523	172.16.0.32	172.16.0.31	Generic data	11:34:12.647180	0.0580040	
524	38AD8E-384AF8	010FE2-000007	Generic data	11:34:12.659280	0.0121000	
525	4437E6-C5C753	010FE2-000007	UDP: Port 58445 => 2649	11:34:12.677810	0.0185220	
526	192.168.233.15	192.168.233.25	UDP: Port 50585 => 2649	11:34:12.759760	0.0819570	
527	74EAC8-D62DCC	010FE2-000007	Generic data	11:34:12.786460	0.0266980	
528	38AD8E-381258	010FE2-000007	Generic data	11:34:12.836120	0.0496560	
529	4437E6-C5C2CD	FFFFFFFF-FFFFFF	UDP: Port 137 => 137	11:34:12.868160	0.0320280	
530	192.168.233.14	192.168.233.25	NetBios_Name: Request, Transaction ID 37	11:34:12.879880	0.0117290	
531	4437E6-C5C2CD	FFFFFFFF-FFFFFF	UDP: Port 137 => 137			
532	192.168.233.14	192.168.233.25	NetBios_Name: Request, Transaction ID 37			
533	38AD8E-383EF8	010FE2-000007	Generic data			

00000000: 00 0C 29 F7 6E B1 00 0C 29 1A CD FD 08 00 45 00 ..)=n+..).Iy..E.
00000010: 00 33 35 E0 40 00 80 06 6C 85 AC 10 00 20 AC 10 .35a8...l...~.
00000020: 00 1F 04 27 00 15 2C F4 34 2B F7 3C 2F 9F 50 18,64+</.P.
00000030: FA E0 91 44 00 00 50 41 53 53 20 31 39 32 38 0D na.D..PASS 1928.
00000040: 0A

Ethernet 802.3

Ethernet

MAC Destination = 000C29-F76EB1 Unicast address

MAC Source = 000C29-1ACDFD Unicast address

EtherType = Length = 0800 IP Protocol

Ethernet

IPv4 (Internet Protocol version 4)

IP

Version and Header length

Version = 4

Header length = 20 (field value = 5)

Type of service = 00

Total length = 51

Identification = 13792

Flags and Fragment offset

Unused = 0.....

Don't fragment = .1.....

More fragments = .0.....

Fragment offset = 0 (field value = 0)

Time to live = 128

Next protocol = 6 TCP Protocol

Header Checksum = 8C05 (correct)

Source address = 172.16.0.32

Destination address = 172.16.0.31

IP

TCP (Transmission Control Protocol)

TCP

Source port = 1063

Destination port = 21 FTP Control Protocol

Sequence number = 754201643

Acknowledgement Number = 4147916703

Header length and Flags

Header length = 20 (field value = 5)

Reserved (must be zero) =000000....

Urgent pointer =0.....

Ack valid =1.....

Push requested =1.....

Reset requested =0.....

Syn requested =0.....

Fin requested =0.....