

警示：实验报告如有雷同，雷同各方当次实验成绩均以 0 分计；在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计；实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班级	2015 级电子政务	学号	15331191	姓名	廖颖泓
完成日期： 2017 年 12 月 21 日							

FTP 协议分析实验

【实验目的】

分析 FTP 协议的安全性。

【实验步骤】

1. 配置 Serv-U 服务器；建立用户名和密码（用户名是 USER，密码 PASS）；
(有很多可参考的网络资源。比如 <http://www.jb51.net/article/28530.htm>)
2. 使用协议分析软件 Wireshark (<http://www.wireshark.org/download.html>)，设置好过滤规则为 ftp。
3. 客户端使用 ftp 命令访问服务器端，输入用户名和密码。
4. 开始抓包，从捕获的数据包中分析用户名/口令 (请在截图上标出)。
5. 讨论 FTP 协议的安全问题。

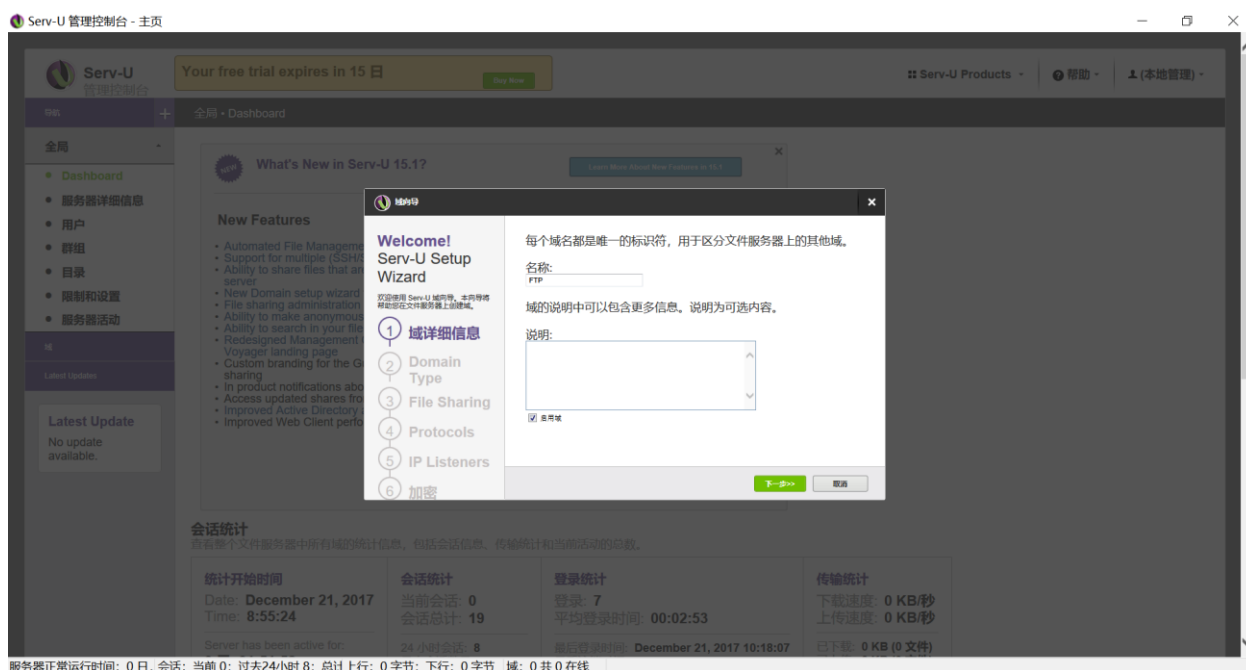
6. 设置 Serv-U 的安全连接功能，客户端使用 (1) http (2) https (3) FileZilla 或 cutFTP，重复步骤 2-4，看是否能保证用户名/口令的安全？

【实验工具】

使用 Wireshark 可以很方便地对截获的数据包进行分析，包括该数据包的源地址、目的地址、所属协议等。Wireshark 的图形化嗅探器界面中，整个窗口被分成三个部分：最上面为数据包列表，用来显示截获的每个数据包的总结性信息；中间为协议树，用来显示选定的数据包所属的协议信息；最下边是以十六进制形式表示的数据包内容，用来显示数据包在物理层上传输时的最终形式。

【实验过程】（要有实验截图）

1. 配置 Serv-U 服务器；建立用户名和密码（用户名是 USER，密码 PASS）；



域向导

Welcome!

Serv-U Setup Wizard

欢迎使用 Serv-U 域向导。本向导将帮助您在文件服务器上创建域。

1 域详细信息

2 Domain Type

3 File Sharing

4 Protocols

5 IP Listeners

6 加密

The File Sharing feature allows your domain users to send or receive files from guests. Use the options below to configure this feature.

Domain URL (ex. "www.mysite.com" or "127.0.0.1"):

127.0.0.1

File Sharing Repository:

/E:/share

☐ Use Secure URL (HTTPS)

配置 SMTP...

<< 上一步

下一步 >>

取消

域向导

Welcome!

Serv-U Setup Wizard

欢迎使用 Serv-U 域向导。本向导将帮助您在文件服务器上创建域。

1 域详细信息

2 Domain Type

3 File Sharing

4 Protocols

5 IP Listeners

6 加密

可以使用域通过各种协议提供对文件服务器的访问。如果当前许可证不支持某些协议，则这些协议可能无法使用。请选择域应该使用的协议及其相应的端口。

<input checked="" type="checkbox"/> FTP 和 Explicit SSL/TLS	21
<input checked="" type="checkbox"/> Implicit FTPS (SSL/TLS)	990
<input checked="" type="checkbox"/> 使用 SSH 的 SFTP	22
<input checked="" type="checkbox"/> HTTP	80
<input checked="" type="checkbox"/> HTTPS (SSL 加密的 HTTP)	443

<< 上一步

下一步 >>

取消

域向导

Welcome!

Serv-U Setup Wizard

欢迎使用 Serv-U 域向导。本向导将帮助您在文件服务器上创建域。

1 域详细信息

2 Domain Type

3 File Sharing

4 Protocols

5 IP Listeners

6 加密

IP 地址指定了一个地址，域应对该地址的请求连接进行监听。

IPv4 地址:

<< 所有可用的 IPv4 地址 >>

☒ 创建 IPv4 监听器

IPv6 地址:

<< 所有可用的 IPv6 地址 >>

☒ 创建 IPv6 监听器

<< 上一步

下一步 >>

取消

配置 Serv-U 服务器

用户向导 - 步骤 1 总步骤 4

×



欢迎使用 Serv-U 用户账户向导。该向导帮助您快速创建新用户，以访问您的文件服务器。

客户端尝试登录文件服务器时通过登录 ID 标识其账户。

登录 ID:

USER

全名:

(可选)

电子邮件地址:

(可选)

下一步 >>

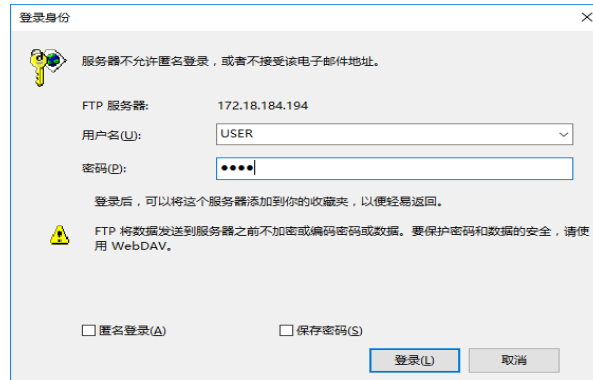
取消

设置用户名

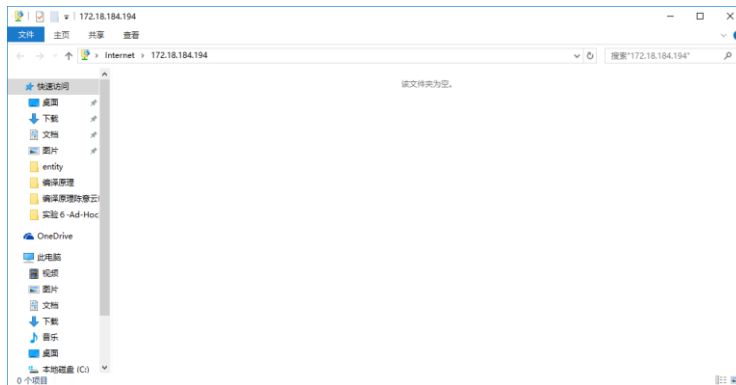
设置密码

添加用户成功

FTP 服务器正在监听

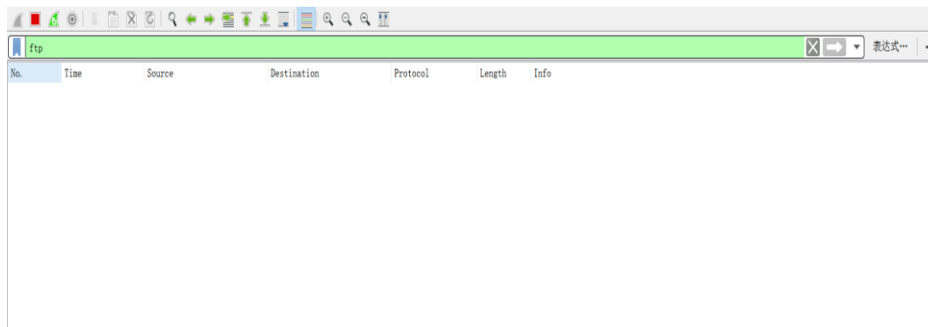


用户名和密码登录 FTP 服务器



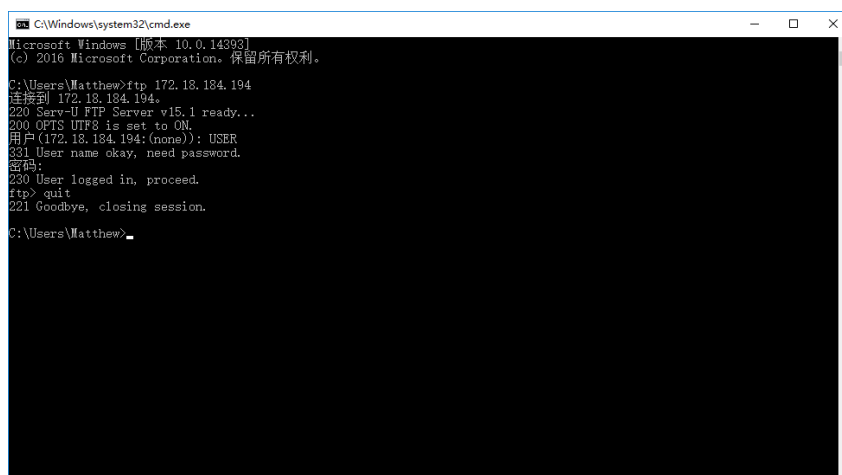
登录 FTP 服务器成功

2. 使用协议分析软件 Wireshark, 设置好过滤规则为 ftp。



过滤规则为 ftp

3. 客户端使用 ftp 命令访问服务器端, 输入用户名和密码。



客户端使用 ftp 命令访问服务器端，输入用户名 USER 和密码 PASS

4. 开始抓包，从捕获的数据包中分析用户名/口令 (请在截图上标出)。

No.	Time	Source	Destination	Protocol	Length	Info
327	19.463568	172.18.184.194	172.18.184.153	FTP	92	Response: 220 Serv-U FTP Server v15.1 ready...
331	19.471777	172.18.184.153	172.18.184.194	FTP	68	Request: OPTS UTF8 ON
332	19.472821	172.18.184.194	172.18.184.153	FTP	83	Response: 200 OPTS UTF8 is set to ON.
440	23.863996	172.18.184.153	172.18.184.194	FTP	65	Request: USER USER
441	23.868491	172.18.184.194	172.18.184.153	FTP	90	Response: 331 User name okay, need password.
625	28.312701	172.18.184.153	172.18.184.194	FTP	65	Request: PASS PASS
626	28.316289	172.18.184.194	172.18.184.153	FTP	84	Response: 230 User logged in, proceed.
695	35.463838	172.18.184.153	172.18.184.194	FTP	60	Request: QUIT
696	35.465178	172.18.184.194	172.18.184.153	FTP	85	Response: 221 Goodbye, closing session.

Frame 441: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
 Ethernet II, Src: Dell_5a:18:ca (b0:83:fe:5a:18:ca), Dst: Dell_81:78:a7 (a4:1f:72:81:78:a7)
 Internet Protocol Version 4, Src: 172.18.184.194, Dst: 172.18.184.153
 Transmission Control Protocol, Src Port: 21, Dst Port: 50227, Seq: 68, Ack: 26, Len: 36
 File Transfer Protocol (FTP)
 331 User name okay, need password.\r\n
 Response code: User name okay, need password (331)
 Response arg: User name okay, need password.

捕获的数据包中分析出用户名 USER

Time	Source	Destination	Protocol	Length	Info
327	19.463568	172.18.184.194	FTP	92	Response: 220 Serv-U FTP Server v15.1 ready...
331	19.471777	172.18.184.153	FTP	68	Request: OPTS UTF8 ON
332	19.472821	172.18.184.194	FTP	83	Response: 200 OPTS UTF8 is set to ON.
440	23.863996	172.18.184.153	FTP	65	Request: USER USER
441	23.868491	172.18.184.194	FTP	90	Response: 331 User name okay, need password.
625	28.312701	172.18.184.153	FTP	65	Request: PASS PASS
626	28.316289	172.18.184.194	FTP	84	Response: 230 User logged in, proceed.
695	35.463838	172.18.184.153	FTP	60	Request: QUIT
696	35.465178	172.18.184.194	FTP	85	Response: 221 Goodbye, closing session.

Frame 625: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
 Ethernet II, Src: Dell_81:78:a7 (a4:1f:72:81:78:a7), Dst: Dell_5a:18:ca (b0:83:fe:5a:18:ca)
 Internet Protocol Version 4, Src: 172.18.184.153, Dst: 172.18.184.194
 Transmission Control Protocol, Src Port: 50227, Dst Port: 21, Seq: 26, Ack: 104, Len: 11
 File Transfer Protocol (FTP)
 PASS PASS\r\n
 Request command: PASS
 Request arg: PASS

捕获的数据包中分析出口令 PASS

5. 讨论 FTP 协议的安全问题。

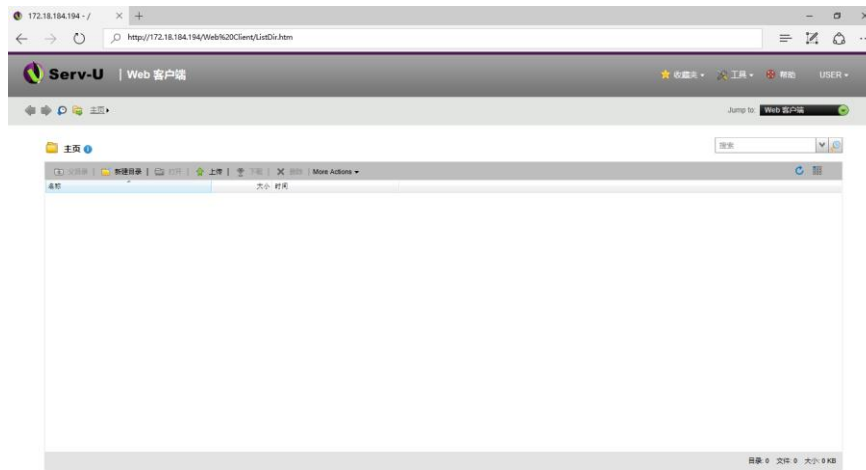
TCP/IP 协议族的设计是在相互信任和安全的基础上进行的，FTP 的设计因此没有采用加密传送。于是 FTP 客户端与服务器之前所有的数据都是通过明文的方式传送，其中就包括口令。从有了交换环境下的数据监听之后，这种明文传送就变得十分危险，因为别人可能从传输过程过捕获一些敏感的信息，如用户名和口令等，这样黑客就可以通过捕获 FTP 的用户名和口令来取得主机系统的账号，如果该账号可以远程登录的话，通常采用本地溢出来获得 root 权限，这台 FTP 服务器就被黑客控制了。

6. 设置 Serv-U 的安全连接功能，客户端使用 (1) http (2) https (3) FileZilla 或 cutFTP，重复步骤2-4，看是否能保证用户名/口令的安全？

(1) http



客户端使用 http 通过用户名和密码登录 FTP 服务器



客户端使用 http 通过用户名和密码成功登录上 FTP 服务器

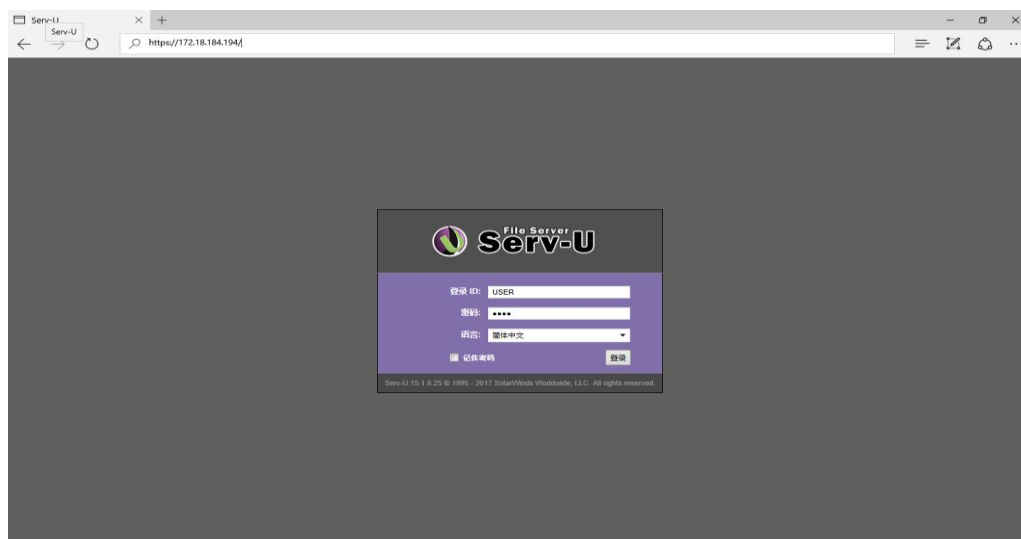
No.	Time	Source	Destination	Protocol	Length	Info
1433	23.332391	172.18.184.194	172.18.184.153	HTTP	531	HTTP/1.0 304 Not Modified
1438	23.333299	172.18.184.194	172.18.184.153	HTTP	531	HTTP/1.0 304 Not Modified
1448	23.339206	172.18.184.153	172.18.184.194	HTTP	570	GET /Common/Images/su16x16.png HTTP/1.1
1451	23.340033	172.18.184.153	172.18.184.194	HTTP	575	GET /Common/Images/WebClient16.png HTTP/1.1
1454	23.349271	172.18.184.194	172.18.184.153	HTTP	531	HTTP/1.0 304 Not Modified
1457	23.350116	172.18.184.194	172.18.184.153	HTTP	531	HTTP/1.0 304 Not Modified
1597	30.796919	172.18.184.153	1.192.137.248	HTTP	1257	POST /qexquery HTTP/1.1
1599	30.827456	1.192.137.248	172.18.184.153	HTTP	445	HTTP/1.1 200 OK (application/octet-stream)
1612	31.371021	172.18.184.153	172.18.184.194	HTTP	103	POST /Web%20Client/Login.xml?Command=Login&Sync=1513844314268 HT
1619	31.385129	172.18.184.194	172.18.184.153	HTTP/XML	444	HTTP/1.0 200 OK
1653	33.547437	172.18.184.153	172.18.184.194	HTTP	691	GET /Web%20Client/ListOfDir.htm HTTP/1.1
1699	33.627620	172.18.184.194	172.18.184.153	HTTP	894	HTTP/1.0 200 OK (text/html)
1705	33.628682	172.18.184.153	172.18.184.194	HTTP	675	GET /Common/Style/jquery/jquery-ui.css HTTP/1.1
1710	33.629550	172.18.184.153	172.18.184.194	HTTP	684	GET /Common/Style/jquery/jquery-contextMenu.css HTTP/1.1

Frame 1612: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
 Ethernet II, Src: Dell_81:78:a7 (a4:1f:72:81:78:a7), Dst: Dell_5a:18:ca (b0:83:fe:5a:18:ca)
 Internet Protocol Version 4, Src: 172.18.184.153, Dst: 172.18.184.194
 Transmission Control Protocol, Src Port: 59706, Dst Port: 80, Seq: 704, Ack: 1, Len: 49
 [2 Reassembled TCP Segments (752 bytes): #1610(703), #1612(49)]
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "user" = "USER"
 Form item: "pword" = "PASS"
 Form item: "viewshare" = ""
 Form item: "language" = "zh,CN"

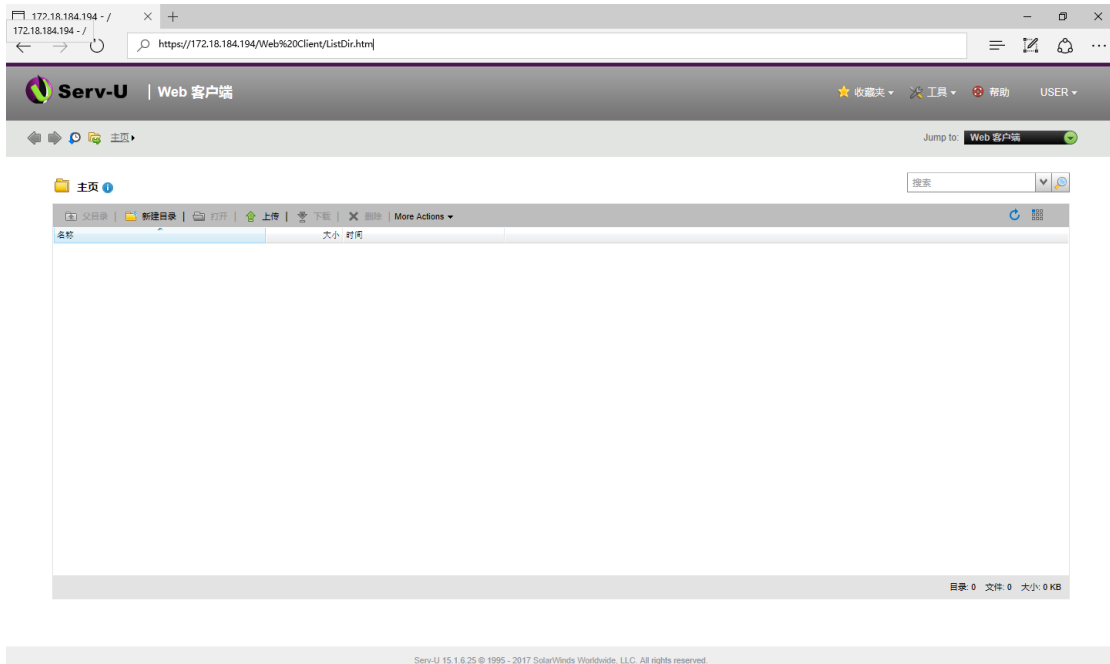
捕获的 http 数据包中分析出用户名 USER 和口令 PASS

http 协议不能保证用户名/口令的安全。

(2) https



客户端使用 https 通过用户名和密码登录 FTP 服务器



客户端使用 https 通过用户名和密码成功登录上 FTP 服务器

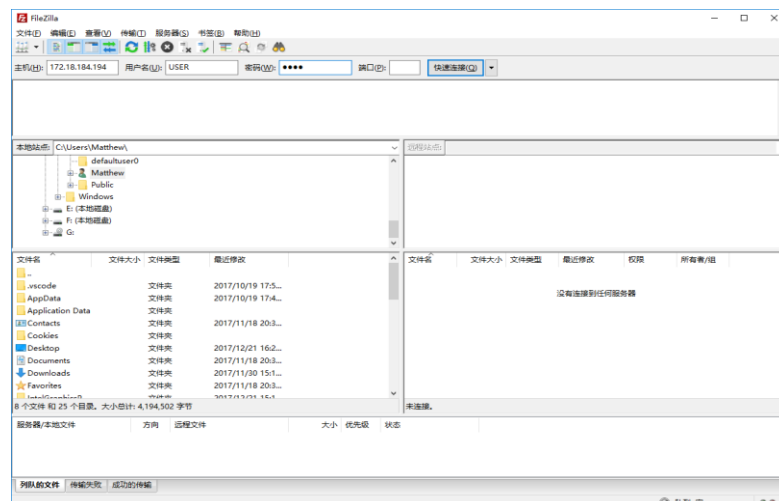
No.	Time	Source	Destination	Protocol	Length	Info
846	8.571356	172.18.184.153	172.18.184.194	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
847	8.572457	172.18.184.153	172.18.184.194	TLSv1.2	790	Application Data
849	8.574095	172.18.184.194	172.18.184.153	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
852	8.574449	172.18.184.153	172.18.184.194	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
853	8.574921	172.18.184.194	172.18.184.153	TLSv1.2	752	Application Data
854	8.574922	172.18.184.194	172.18.184.153	TLSv1.2	85	Encrypted Alert
858	8.575475	172.18.184.153	172.18.184.194	TLSv1.2	812	Application Data
861	8.577493	172.18.184.194	172.18.184.153	TLSv1.2	752	Application Data
864	8.578291	172.18.184.194	172.18.184.153	TLSv1.2	85	Encrypted Alert
870	8.595953	172.18.184.153	172.18.184.194	TLSv1.2	411	Client Hello
871	8.598369	172.18.184.194	172.18.184.153	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
874	8.598705	172.18.184.153	172.18.184.194	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
875	8.599777	172.18.184.153	172.18.184.194	TLSv1.2	775	Application Data
882	8.602508	172.18.184.194	172.18.184.153	TLSv1.2	1461	Application Data
883	8.602508	172.18.184.194	172.18.184.153	TLSv1.2	85	Encrypted Alert
891	8.610874	172.18.184.153	172.18.184.194	TLSv1.2	411	Client Hello
892	8.616844	172.18.184.194	172.18.184.153	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
894	8.617233	172.18.184.153	172.18.184.194	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message

> Frame 894: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
 > Ethernet II, Src: Dell_81:78:a7 (a4:1f:72:81:78:a7), Dst: Dell_5a:18:ca (b0:83:fe:5a:18:ca)
 > Internet Protocol Version 4, Src: 172.18.184.153, Dst: 172.18.184.194
 > Transmission Control Protocol, Src Port: 59809, Dst Port: 443, Seq: 358, Ack: 106, Len: 51
 > Secure Sockets Layer
 > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

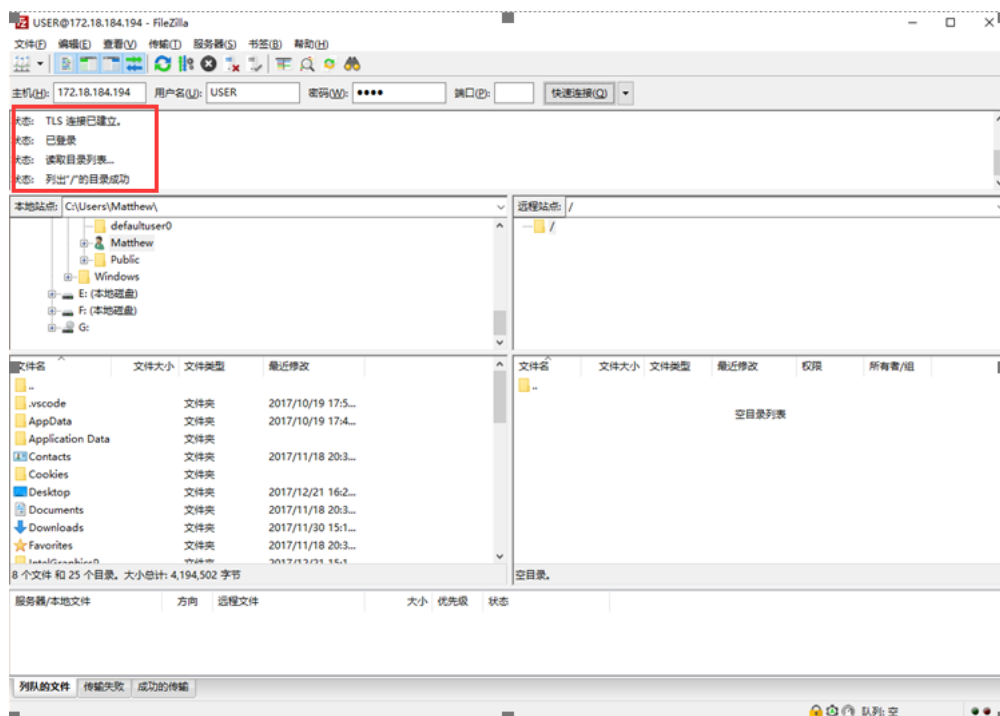
捕获的数据包中分析不出用户名 USER 和口令 PASS

https 通过 SSL 用户名和口令进行加密，使得用户名和口令不会因为数据包捕获而泄露。

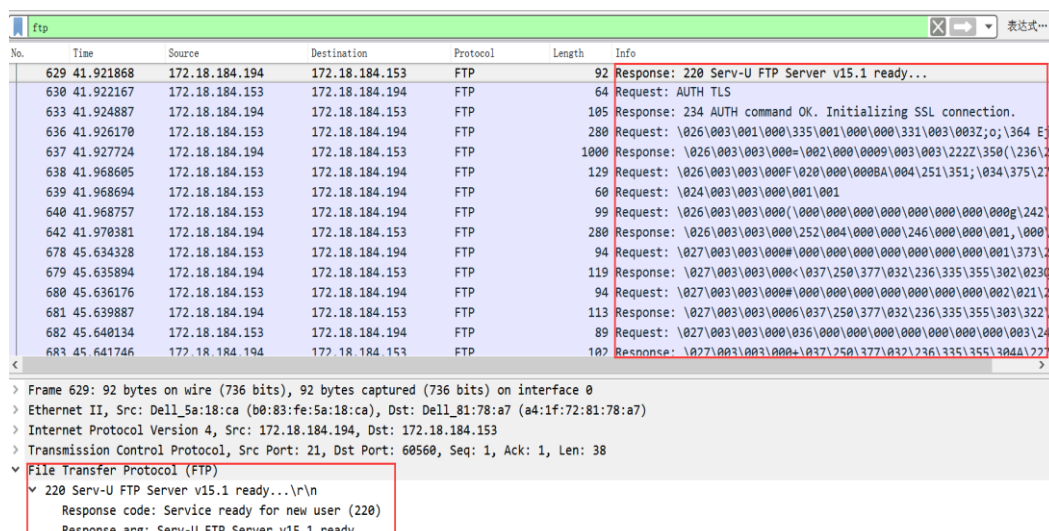
(3) FileZilla



客户端使用 FileZilla 通过用户名和密码登录 FTP 服务器



客户端使用 FileZilla 通过用户名和密码成功登录上 FTP 服务器



捕获的数据包中分析不出用户名 USER 和口令 PASS

FileZilla 通过 TL 对 ftp 报文进行加密，使得用户名和口令不会因为数据包捕获而泄露。

【实验体会】

本次实验通过 Serv-U 搭建 FTP 服务器和用 Wireshark 捕获对 ftp 命令、http、https、FileZilla 四种方式访问 FTP 服务器的登录和访问报文并尝试分析出用户名和口令。结果发现，使用 ftp 命令和 http 两种方式访问 FTP 服务器都很容易在数据包被捕获的情况下导致用户名和口令的泄露。由于 https 协议在原有 http 协议基础上加入了 SSL 层，用户名和口令得以保护使得不会因为数据包被捕获而泄露。FileZilla 则是通过 TLS 协议对 ftp 数据包进行加密，使得用户名和口令不会因为数据包被捕获而泄露。实验结果说明，在访问 FTP 服务器时，为了保证数据的安全，应尽量使用 https 协议或使用像 FileZilla 这样的有安全协议加密报文的 FTP 应用软件访问 FTP 服务器。