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】

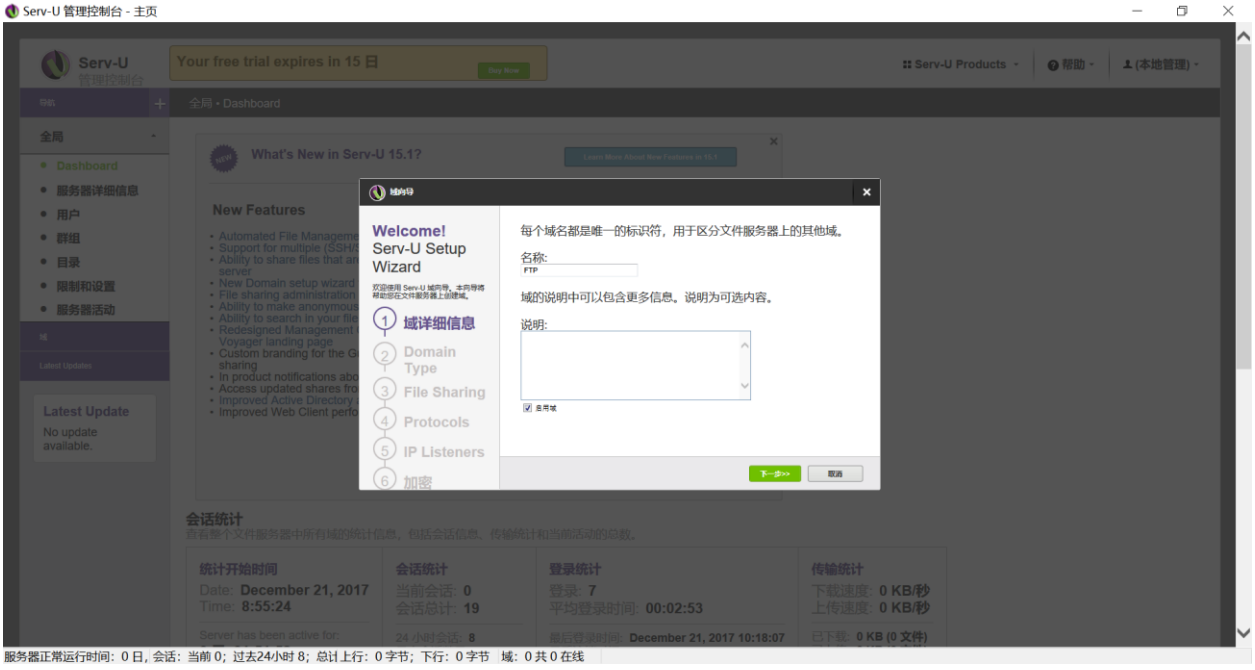
1. 配置 Serv-U 服务器；建立用户名和密码（用户名是USER，密码PASS）；
   (有很多可参考的网络资源。比如 http://www.jb51.net/article/28530.htm)
2. 使用协议分析软件 wireshark (http://www.wireshark.org/download.html)，设置好过滤规则为 ftp。
3. 客户端使用 ftp 命令访问服务器端，输入用户名和密码。
4. 开始抓包，从捕获的数据包中分析用户名/口令 (请在截图上标出)。
5. 讨论 FTP 协议的安全问题。
6. 设置 Serv-U 的安全连接功能，客户端使用 (1) http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

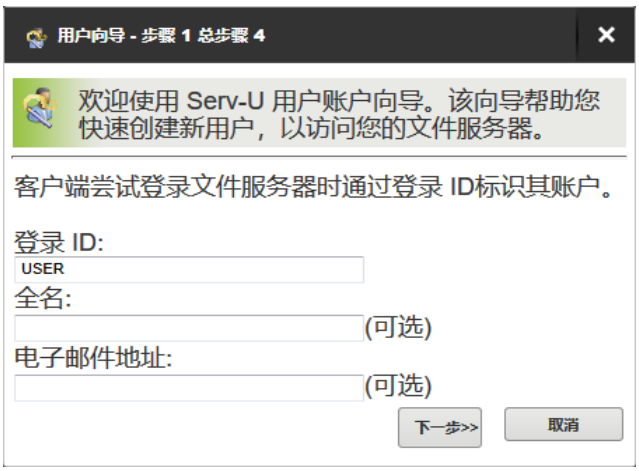
使用 Wireshark 可以很方便地对截获的数据包进行分析，包括该数据包的源地址、目的地址、所属协议等。Wireshark 的图形化嗅探器界面中，整个窗口被分成三个部分：最上面为数据包列表，用来显示截获的每个数据包的总结性信息；中间为协议树，用来显示选定的数据包所属的协议信息；最下边是以十六进制形式表示的数据包内容，用来显示数据包在物理层上传输时的最终形式。

【实验过程】（要有实验截图）

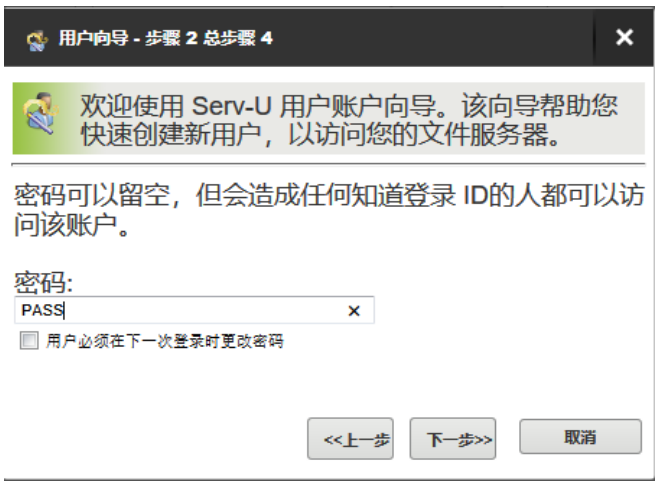
1. 配置 Serv-U 服务器；建立用户名和密码（用户名是USER，密码PASS）；



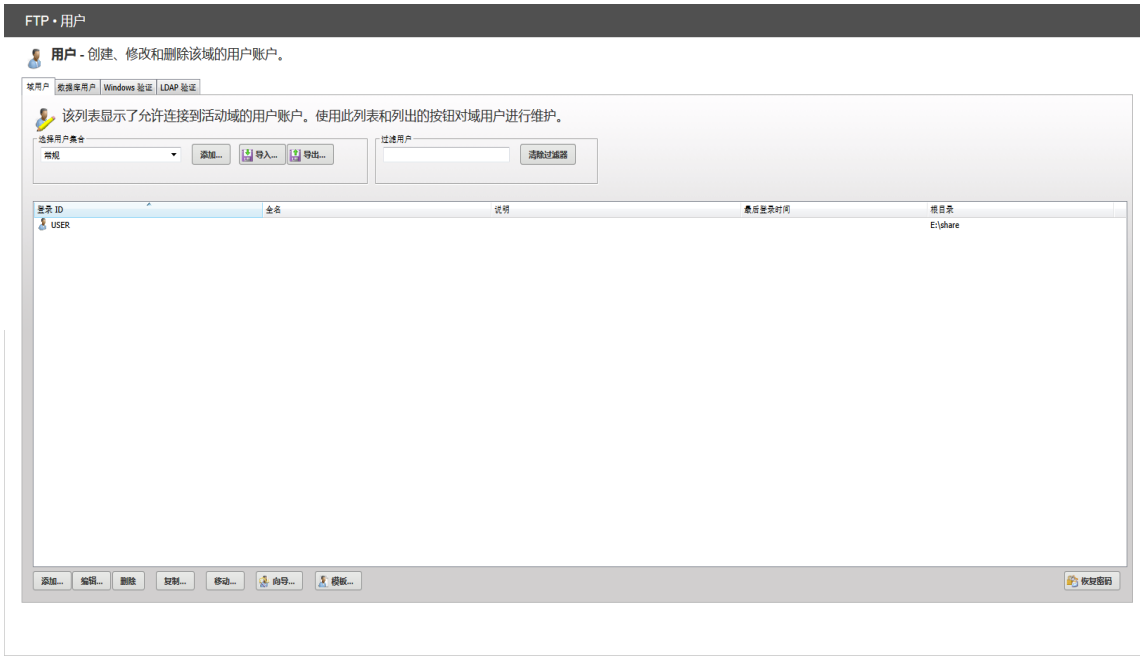
配置 Serv-U 服务器



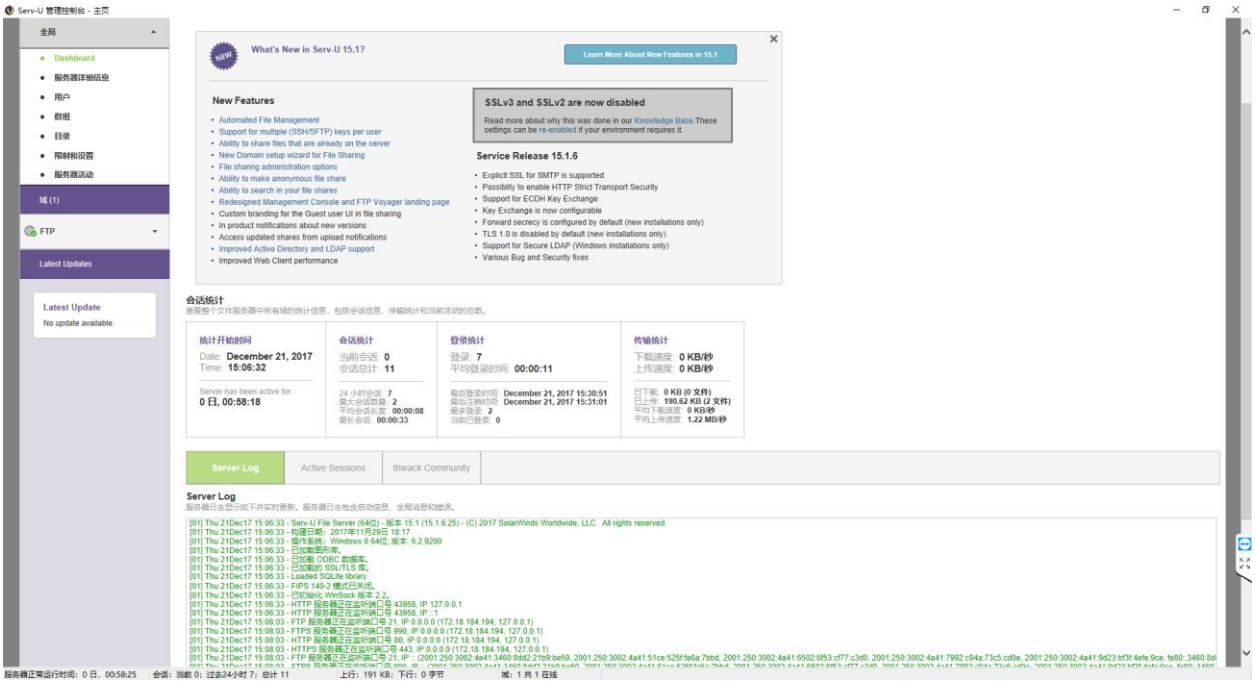
设置用户名



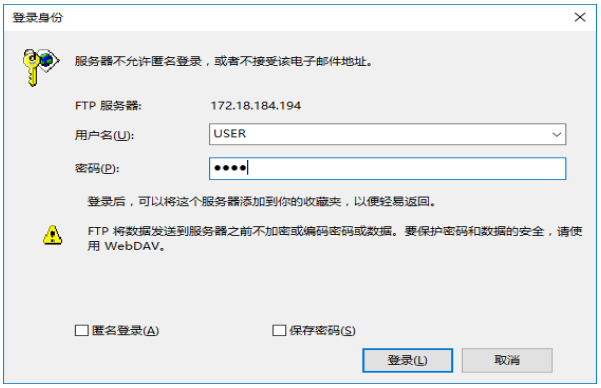
设置密码



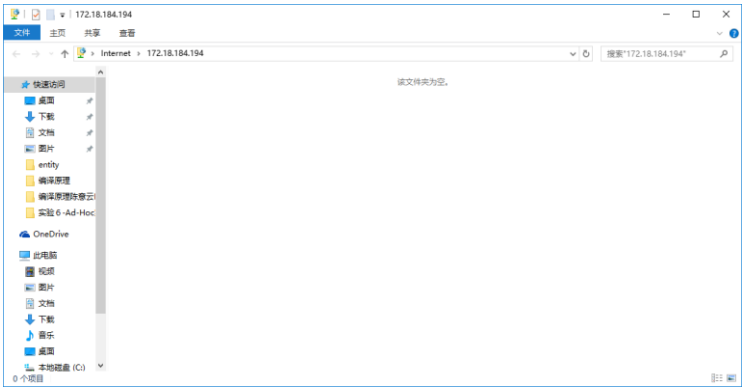
添加用户成功



FTP 服务器正在监听

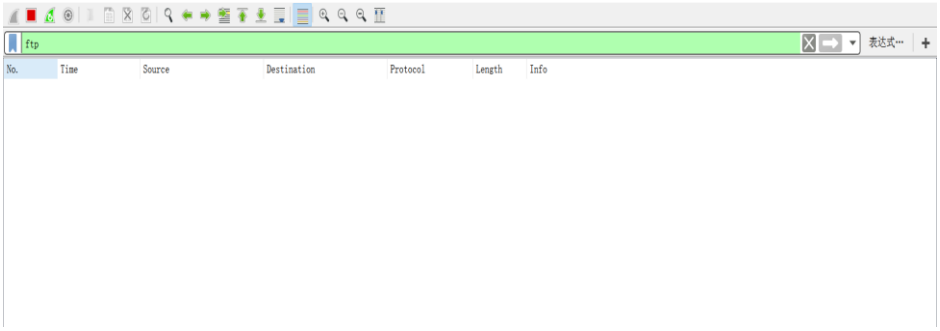


用户名和密码登录 FTP 服务器



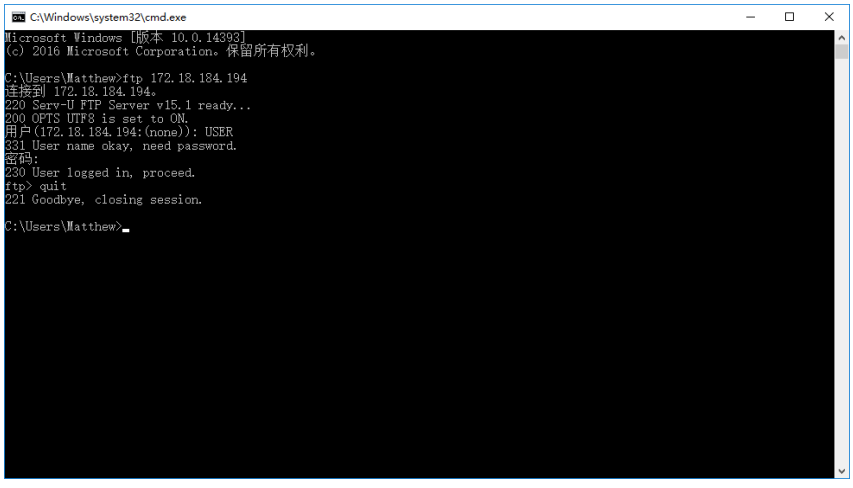
登录 FTP 服务器成功

2. 使用协议分析软件 Wireshark，设置好过滤规则为 ftp。



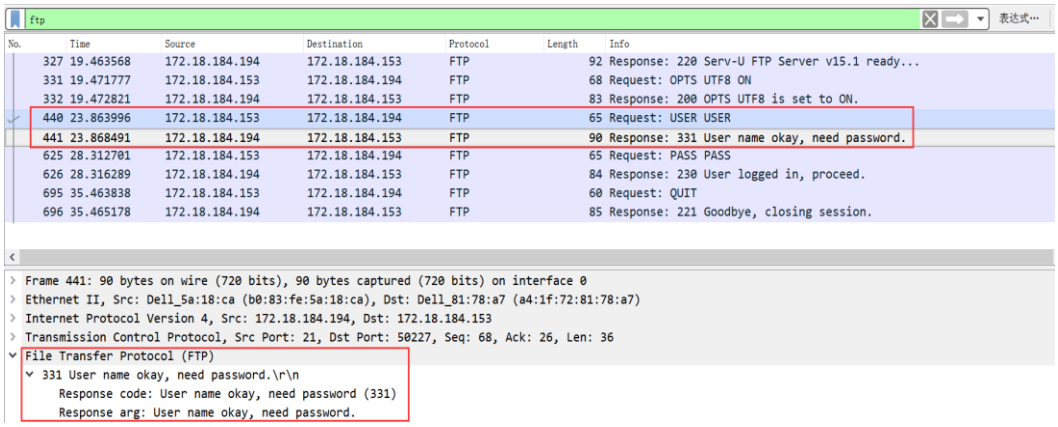
过滤规则为 ftp

3. 客户端使用 ftp 命令访问服务器端，输入用户名和密码。

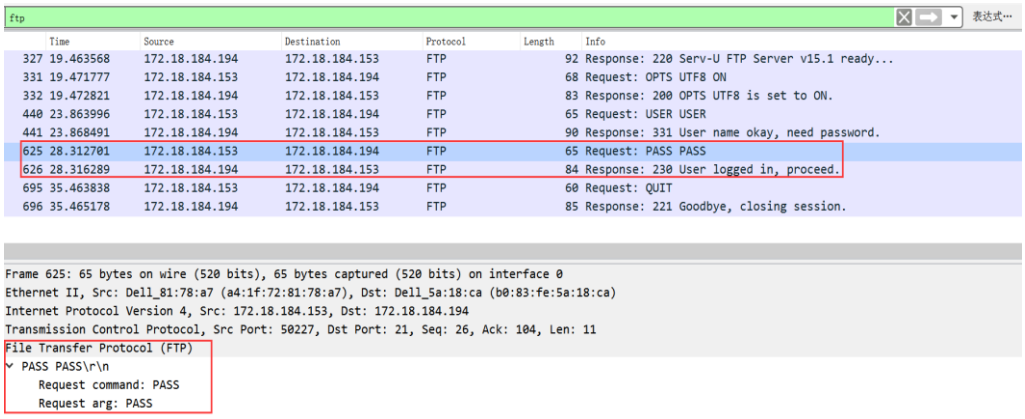


客户端使用 ftp 命令访问服务器端，输入用户名 USER 和密码 PASS

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)。



捕获的数据包中分析出用户名 USER



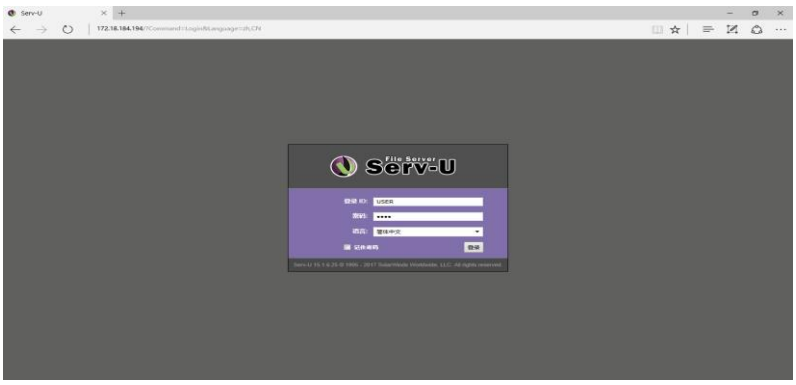
捕获的数据包中分析出口令 PASS

5. 讨论 FTP 协议的安全问题。

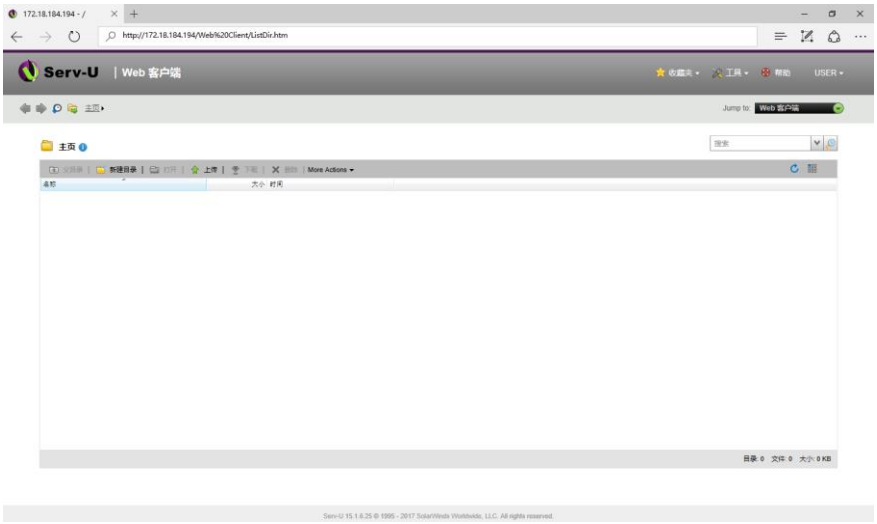
TCP/IP 协议族的设计是在相互信任和安全的基础上进行的，FTP 的设计因此没有采用加密传送。于是 FTP 客户端与服务器之前所有的数据都是通过明文的方式传送，其中就包括口令。从有了交换环境下的数据监听之后，这种明文传送就变得十分危险，因为别人可能从传输过程过捕获一些敏感的信息，如用户名和口令等，这样黑客就可以通过捕获 FTP 的用户名和口令来取得主机系统的账号，如果该账号可以远程登录的话，通常采用本地溢出来获得 root 权限，这台 FTP 服务器就被黑客控制了。

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？

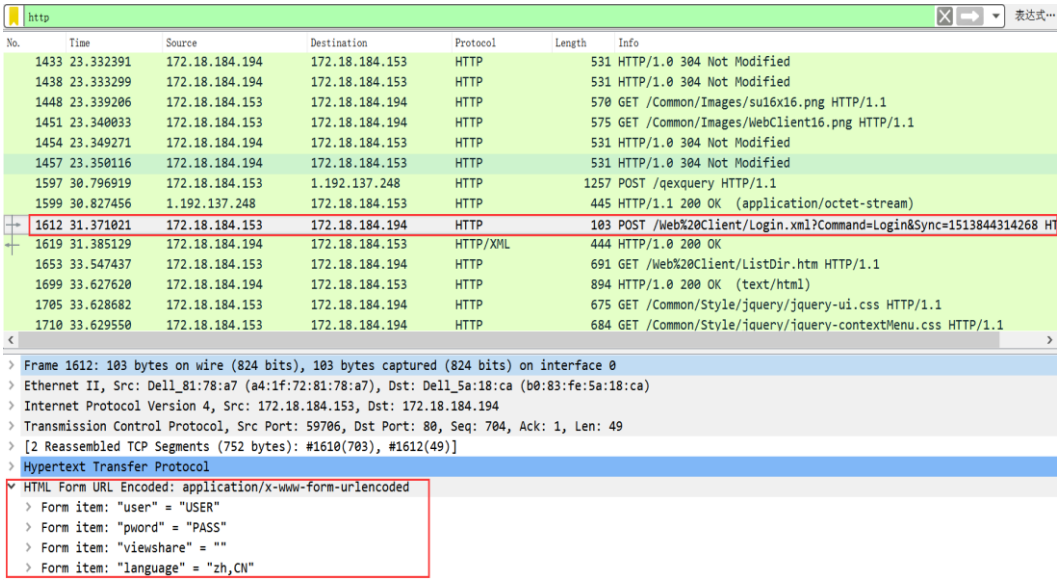
(1) http



客户端使用 http 通过用户名和密码登录 FTP 服务器



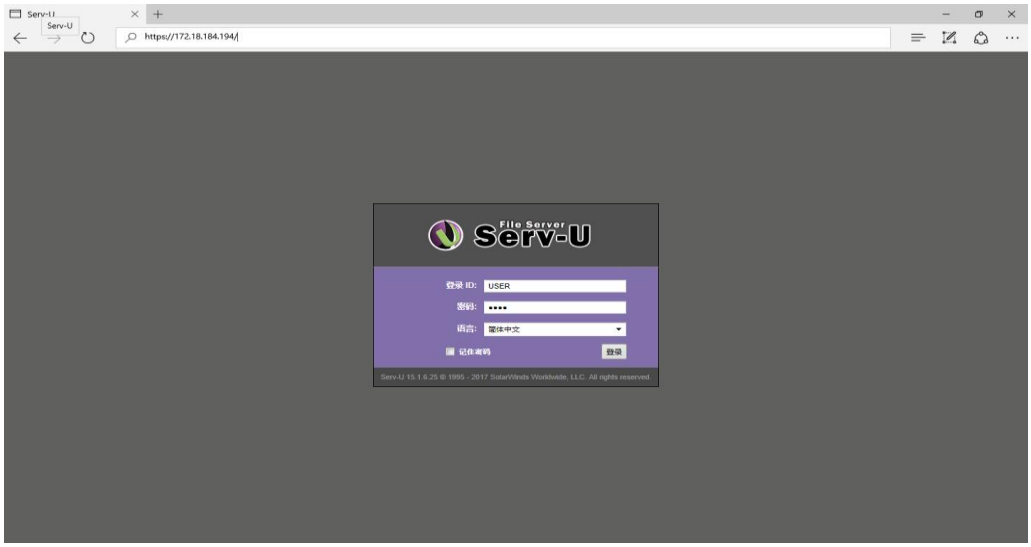
客户端使用 http 通过用户名和密码成功登录上 FTP 服务器



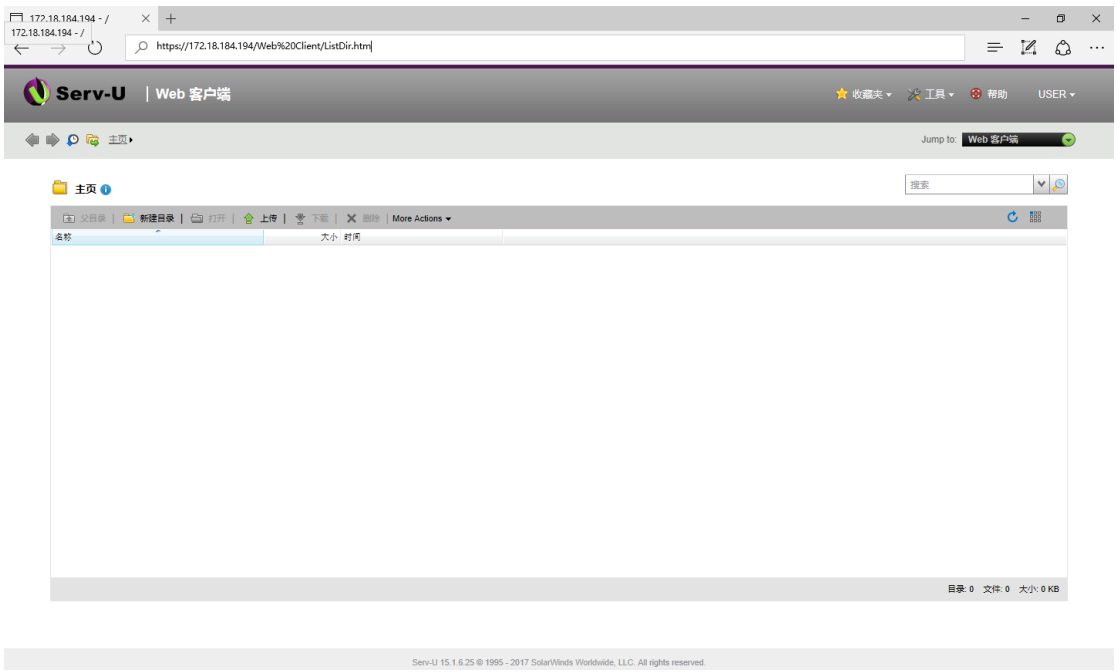
捕获的 http 数据包中分析出用户名 USER 和口令 PASS

http 协议不能保证用户名/口令的安全。

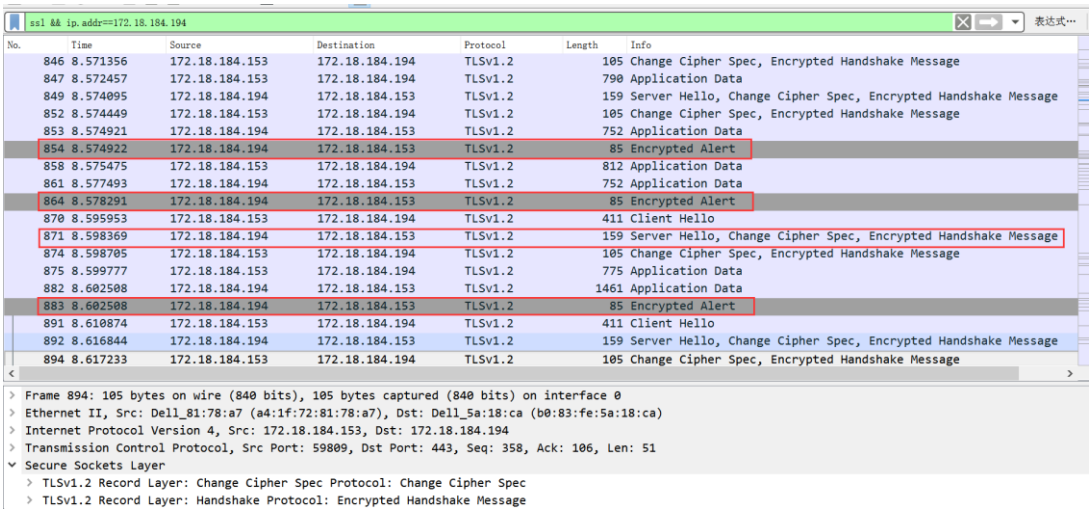
(2) https



客户端使用 https 通过用户名和密码登录 FTP 服务器



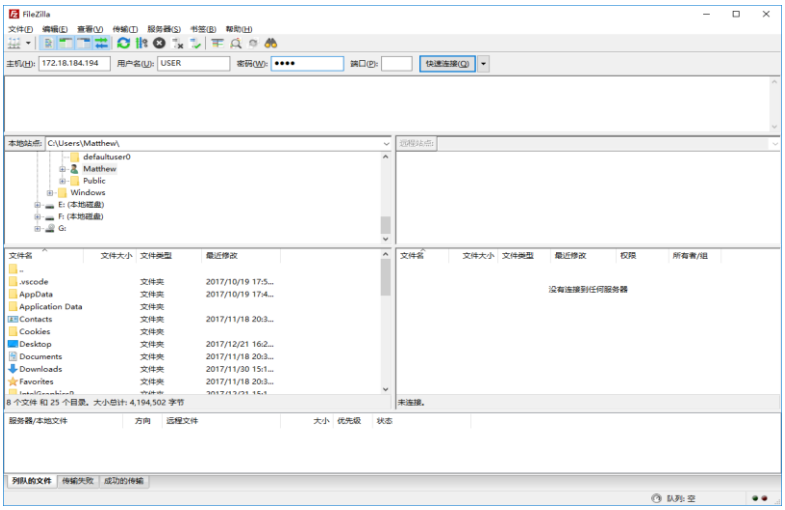
客户端使用 https 通过用户名和密码成功登录上 FTP 服务器



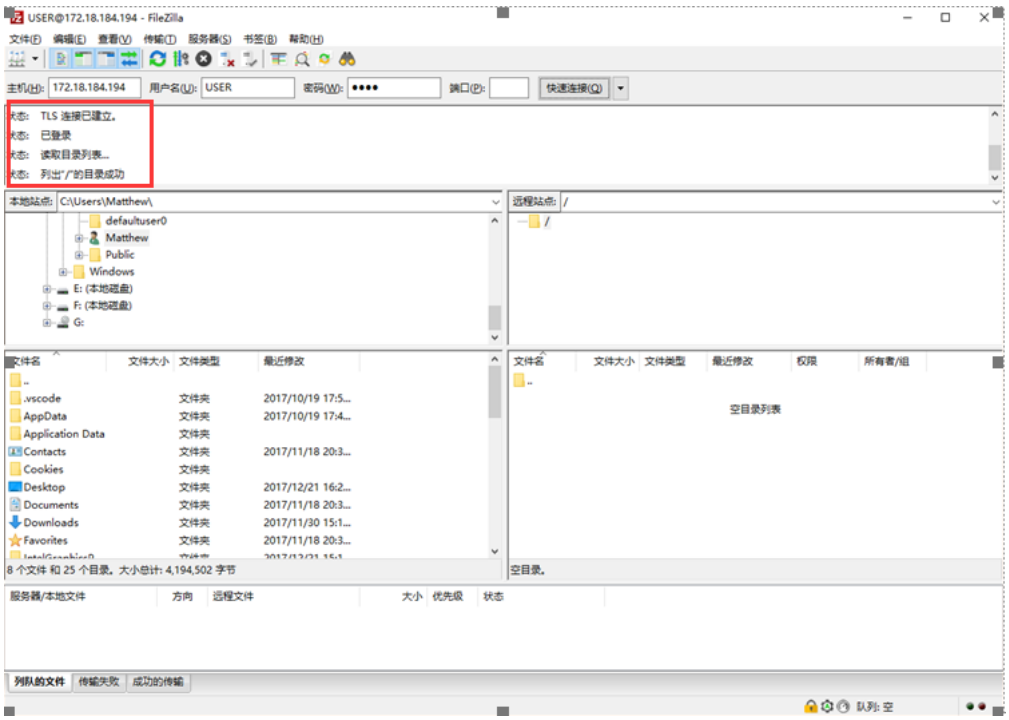
捕获的数据包中分析不出用户名 USER 和口令 PASS

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。

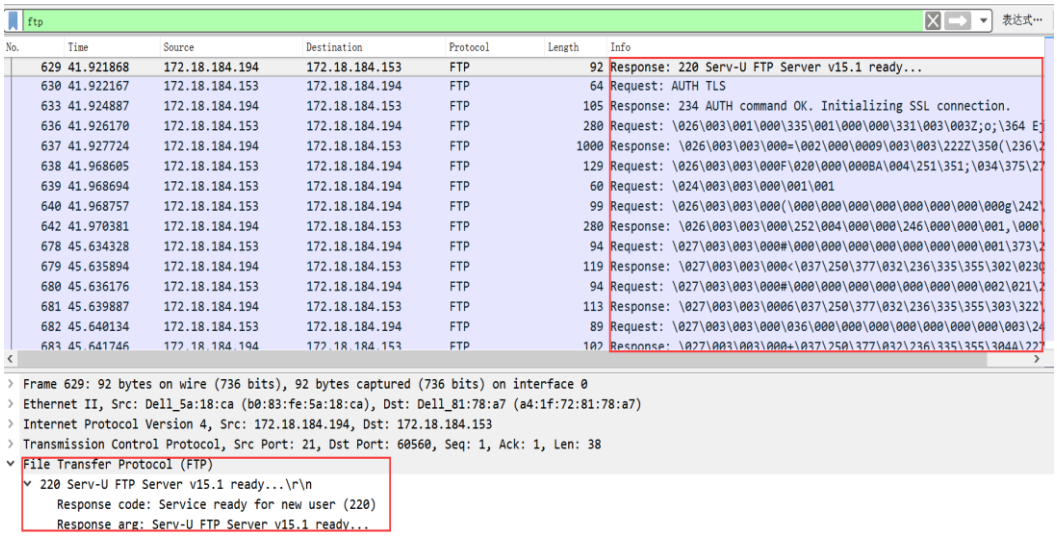
(3) FileZilla



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。