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	周一_3-4_节	学号	15331151	姓名	李佳
完成日期： 2017 年 12 月 19 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】

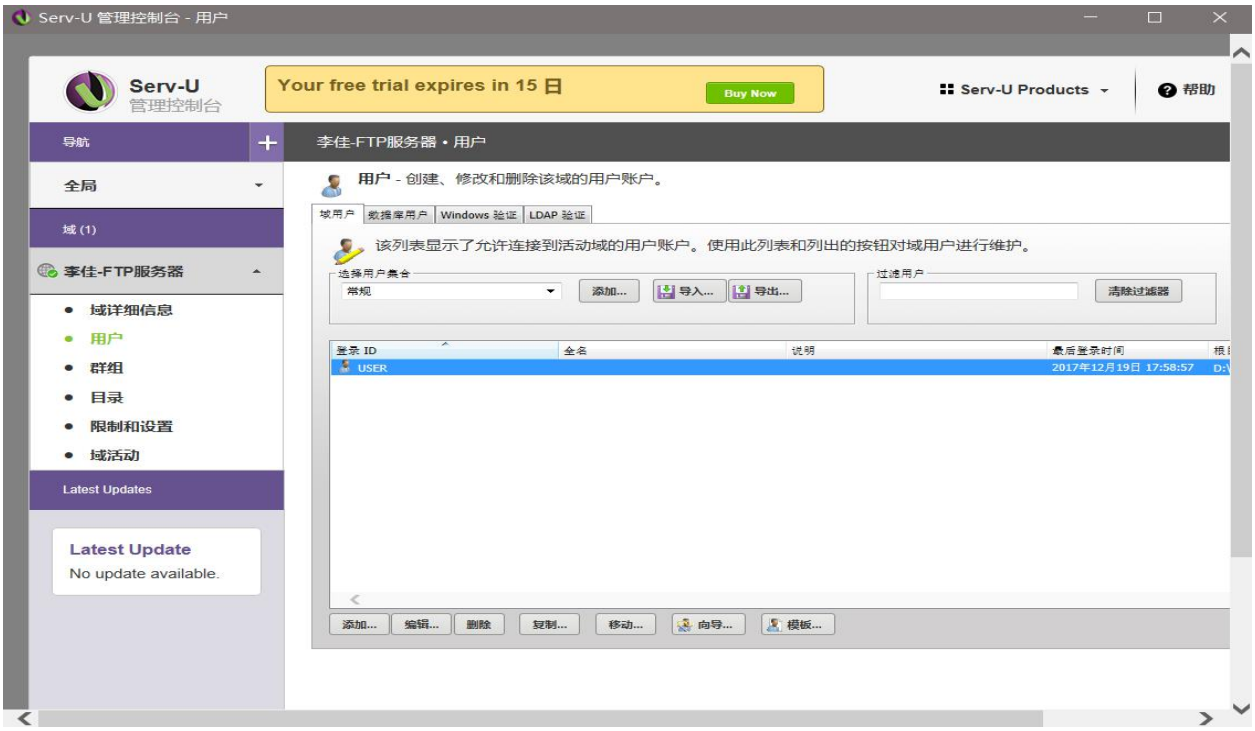
1. 配置 Serv-U 服务器；建立用户名和密码（例如用户名是USER，密码PASS）；
   (有很多可参考的网络资源。比如 http://www.jb51.net/article/28530.htm)
2. 使用协议分析软件 wireshark (http://www.wireshark.org/download.html)，设置好过滤规则为 ftp（安装过程不必截图）。
3. 客户端使用 ftp 命令访问服务器端，输入用户名和密码。
4. 开始抓包，从捕获的数据包中分析用户名/口令 (请在截图上标出)。
5. 讨论 FTP 协议的安全问题。
6. 设置 Serv-U 的安全连接功能，客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



所使用的版本是由 Serv-U 中文网 http://www.serv-u.com.cn/ 下载的，参考安装指南为 https://jingyan.baidu.com/article/e75aca85634b68142edac6f2.html。

2. 使用协议分析软件 wireshark ，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)。

6664	35.2093250	172.18.43.69	172.18.43.171	FTP	92 Response: 220 Serv-U FTP Server v15.1
6666	35.2116700	172.18.43.171	172.18.43.69	FTP	70 Request: USER anonymous
6672	35.2158750	172.18.43.69	172.18.43.171	FTP	124 Response: 331 User name okay, please
6679	35.2187200	172.18.43.171	172.18.43.69	FTP	68 Request: PASS IEUser@
6680	35.2207190	172.18.43.69	172.18.43.171	FTP	95 Response: 530 Sorry, no ANONYMOUS ac
12552	56.7826440	172.18.43.69	172.18.43.171	FTP	92 Response: 220 Serv-U FTP Server v15.1
12555	56.7838870	172.18.43.171	172.18.43.69	FTP	65 Request: USER USER
12556	56.7844530	172.18.43.69	172.18.43.171	FTP	90 Response: 331 User name okay, need p
12558	56.7857780	172.18.43.171	172.18.43.69	FTP	65 Request: PASS PASS
12559	56.7871490	172.18.43.69	172.18.43.171	FTP	84 Response: 230 User logged in, proceed

红色方框为客户机登陆 FTP 服务器所用的用户名和密码，即用户名(USER)和密码(PASS)。

当客户机登陆 FTP 服务器时，首先尝试使用匿名模式进行登陆，因为 FTP 服务器并未开启匿名模式，所以客户机发送命令 USER annoymous 和 PASS IEUser@之后，会收到服务器返回的失败信息。

之后客户机尝试输入用户名和密码，成功进入，服务器返回成功信息，客户机成功登陆到服务器，过程能够被 Wireshark 记录下用户名和密码，从数据包中看出，用户名和密码都是明文。

5. 讨论 FTP 协议的安全问题

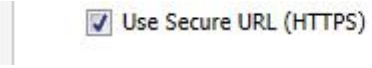
通过上面可以看到 FTP 协议中账户和密码是明文传输的。任何人只要在网络中合适的位置放置一个协议分析仪或者使用嗅探技术就能够看到用户名和口令了。

FTP 对于发送的数据也是以明文的方式进行传输，通过对 FTP 连接的监控和收集数据就可以收集和重现 FTP 的数据传输并实现协议连接回放，进行回放攻击。

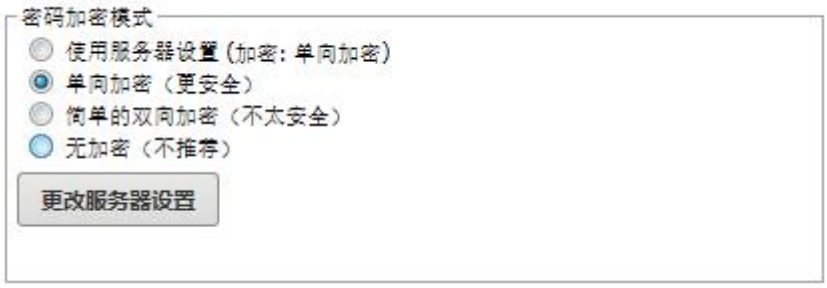
通过第三方软件搭建的 FTP 服务器，黑客可以针对第三方 FTP 服务器使用者进行密码攻击，譬如可以增加一个指向 C 盘的超级管理员用户，提权直接执行命令添加管理员账户，并且添加隐藏的管理员账户，从而实现对主机的完全控制。（来自教程提示）

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？

使用安全 URL，即打开 HTTPS



再使用单向加密：



（1）http 的方式登录到 FTP 服务器

windows 下的会占用 80 端口，所以在建立的时候 HTTP 连接方式的端口需要改一下，不然不能连接。

No.	Time	Source	Destination	Protocol	Length	Info
1426	13.3776010	172.18.43.171	172.18.43.69	TCP	66	5810→80 [SYN] Seq=0 Win=32768 Len=0 MSS=146
1429	13.3814230	172.18.43.69	172.18.43.171	TCP	66	80→5810 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len
1430	13.3818460	172.18.43.171	172.18.43.69	TCP	60	5810→80 [ACK] Seq=1 Ack=1 Win=32768 Len=0
1431	13.3828780	172.18.43.69	172.18.43.171	TCP	54	[TCP Window Update] 80→5810 [ACK] Seq=1 Ack
1680	16.3691720	172.18.43.171	172.18.43.69	TCP	66	5808→80 [SYN] Seq=0 Win=32768 Len=0 MSS=146
1681	16.3692870	172.18.43.69	172.18.43.171	TCP	66	80→5808 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len
1682	16.3695910	172.18.43.171	172.18.43.69	TCP	60	5808→80 [ACK] Seq=1 Ack=1 Win=32768 Len=0
1683	16.3702500	172.18.43.171	172.18.43.69	HTTP	534	GET / HTTP/1.1

从打开网页到成功登入到 FTP 服务器当中，没有发现用户名和口令相关信息，所有数据也不会明文传送，通过 http 的方式能够保障用户名和口令的安全。

（2）https 的方式登录到 FTP 服务器

172.18.43.69	TLSv1.2	242	Client Hello
172.18.43.69	TCP	60	6249→443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
172.18.43.69	TLSv1.2	242	Client Hello
172.18.43.171	TLSv1.2	1000	Server Hello, Certificate, Server Key Exchange, Server Hello Done
172.18.43.171	TCP	54	[TCP Window Update] 443→6248 [ACK] Seq=947 Ack=189 Win=10485760 Len=0
172.18.43.171	TLSv1.2	1000	Server Hello, Certificate, Server Key Exchange, Server Hello Done
172.18.43.171	TCP	54	[TCP Window Update] 443→6249 [ACK] Seq=947 Ack=189 Win=10485760 Len=0
172.18.43.69	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
172.18.43.171	TLSv1.2	280	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
172.18.43.69	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
172.18.43.171	TLSv1.2	280	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

通过 HTTPS 的方式客户机与服务器建立连接时，进行加密解密，没有看到明文的用户名和口令，数据也不是明文进行传输，所以通过 HTTPS 的方式登录到 FTP 服务器，对于用户名和口令来说，也是安全的。

（3）FileZilla 的方式登录到 FTP 服务器

No.	Time	Source	Destination	Protocol	Length	Info
2629	24.3302540	172.18.43.69	172.18.42.253	FTP	104	Response: 220 Serv-U FTP Server v15.1
2631	24.3335620	172.18.42.253	172.18.43.69	FTP	77	Request: USER USER
2632	24.3341320	172.18.43.69	172.18.42.253	FTP	102	Response: 331 User name okay, need pas
2638	24.3369030	172.18.42.253	172.18.43.69	FTP	77	Request: PASS PASS
2639	24.3384420	172.18.43.69	172.18.42.253	FTP	96	Response: 230 User logged in, proceed.

通过 filezilla 客户端登录 FTP 使用 FTP 协议，用户名和口令明文传输，数据同样也是，因此无法保障用户名和口令的安全。

【实验体会】

本次实验过程中建立 FTP 服务器和 Wireshark 抓包在计网实验课上已经学习和进行实践过了，所以没有太大问题。但是在使用 HTTP 登录时出现了问题，一直无法登录，最后在网上找到一些资料中说到 IIS 服务会占用 80 端口，而我建立的也在 80 端口会冲突，所以就要把端口改掉。

通过本次 FTP 协议分析实验，我看到了 FTP 协议的一些优点，比如它在局域网内部使用起来很方便快捷，上传下载文件也很快；比起网络共享来说，它还可以详细设置每个用户的权限。但是它也有很多缺点，首先就是数据以及用户信息的明文传输，这会造成很大的安全隐患，大型或者重要场合就不能使用它进行文件传输，而 HTTP 或者 HTTPS 就相对安全；而且它与防火墙的工作不同步，如果 FTP 客户端 IP 地址不可路由，或者位于防火墙之后，那么就只能使用被动传输模式进行数据传输，如果服务器端的 IP 地址也不可路由，或者位于防火墙之后 FTP 将无法进行数据传输。