信息安全实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.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。
4.实验报告文件以 PDF 格式提交。

院系	数据科学与计算机实验	班 级	14M3，14C1	组长	白冰
学号	14353355	14353002			
学生	杨金华	白冰			
实验分工					
杨金华	编写客户端程序，运行文件，共同编写实验报告	白冰	分析实验结果，共同编写实验报告		

SSL 分析实验

【实验目的】

（1）了解 SSL 工作原理。

（2）通过抓取数据包，了解客户端与 Web 服务端的实际工作流。

【实验环境】

本地主机 IP 地址：172.16.11.1（客户端）。

访问百度：https://www.baidu.com。

【实验说明】

实验可以在 Linux 环境也可以在 Windows 环境。

你的实验环境是：Windows10 。

【实验分析】

1.启动抓包工具 Wireshark。

2.访问 https://www.baidu.com。

3.分析 SSL 协议：

第一阶段：建立起安全协商

客户端向服务端发送自身使用的 SSL 版本、加密算法的相关配置、随机数据以及其在在 SSL 协议中需要用到的信息。服务器反馈给客户端自己的 SSL 版本、加密算法的相关配置、随机数据以及用自己的私有密钥加密的 SERVER-HELLO 信息。服务端紧接着将自己的证书（包含公共密钥）传递过去。

信息安全实验报告

172.16.11.1	203.208.40.39	TCP	66 1753→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PER
203.208.40.39	172.16.11.1	TCP	66 443→1753 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1448 S
172.16.11.1	203.208.40.39	TCP	54 1753→443 [ACK] Seq=1 Ack=1 Win=66608 Len=0
172.16.11.1	203.208.40.39	TLSv1.2	274 Client Hello

第二阶段：服务器鉴别和密钥交换

Server hello:服务端返回协商的信息结果，包括选择使用的协议版本，选择的加密套件、选择的压缩算法、随机数等，其中随机数用于后续的密钥协商;

server_certificates: 服务器端配置对应的证书链，用于身份验证与密钥交换;

server_hello_done:通知客户端 server_hello 信息发送结束;

203.208.40.39	172.16.11.1	TLSv1.2	1502 Server Hello
203.208.40.39	172.16.11.1	TCP	654 [TCP segment of a reassembled PDU]
203.208.40.39	172.16.11.1	TCP	1502 [TCP segment of a reassembled PDU]
203.208.40.39	172.16.11.1	TLSv1.2	409 CertificateServer Key Exchange, Server Hello Done

第三阶段：客户鉴别和密钥交换

client_key_exchange: 合法性验证通过之后，客户端计算产生随机数字 Pre-master，并用证书公钥加密，发送给服务器;

change_cipher_spec，客户端通知服务器后续的通信都采用协商的通信密钥和加密算法进行加密通信;

172.16.11.1	203.208.40.39	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request

第四阶段：结束

双方用 mastersecret 一起产生真正的 sessionkey，这将是一个对称加密的 key。这个 key 还可以用来验证数据完整性。双方再交换结束信息。握手结束。

203.208.40.39	172.16.11.1	TLSv1.2	316 New Session Ticket, Change Cipher Spec, Hello Request, Hello Request

【实验总结】

本次实验为 SSL 分析实验，由于之前并没有学习过相关的知识，而且概念比较抽象，所以做起来会比较难。但通过组员之间的协作，查阅了很多资料，才最终完成实验。

【实验讨论】

SSL: （Secure Socket Layer，安全套接字层），为 Netscape 所研发，用以保障在 Internet 上数据传输之安全，利用数据加密(Encryption)技术，可确保数据在网络上之传输过程中不会被截取。

信息安全实验报告

SSL 协议分为两部分：Handshake Protocol 和 Record Protocol。其中 Handshake Protocol 用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全的协商出一份密钥。 Record Protocol 则定义了传输的格式。

通过抓包分析了 SSL 协议的流程图，对 SSL 协议有了初步了解.

【交实验报告】

上传实验报告：ftp://222.200.180.109/　　截止日期：一周之内完成

上传小组实验报告。上传文件名格式：小组号_防火墙分析实验.pdf （由组长负责上传）

例如: 文件名“6_防火墙管理实验.pdf”表示第 6 组的防火墙分析实验报告。