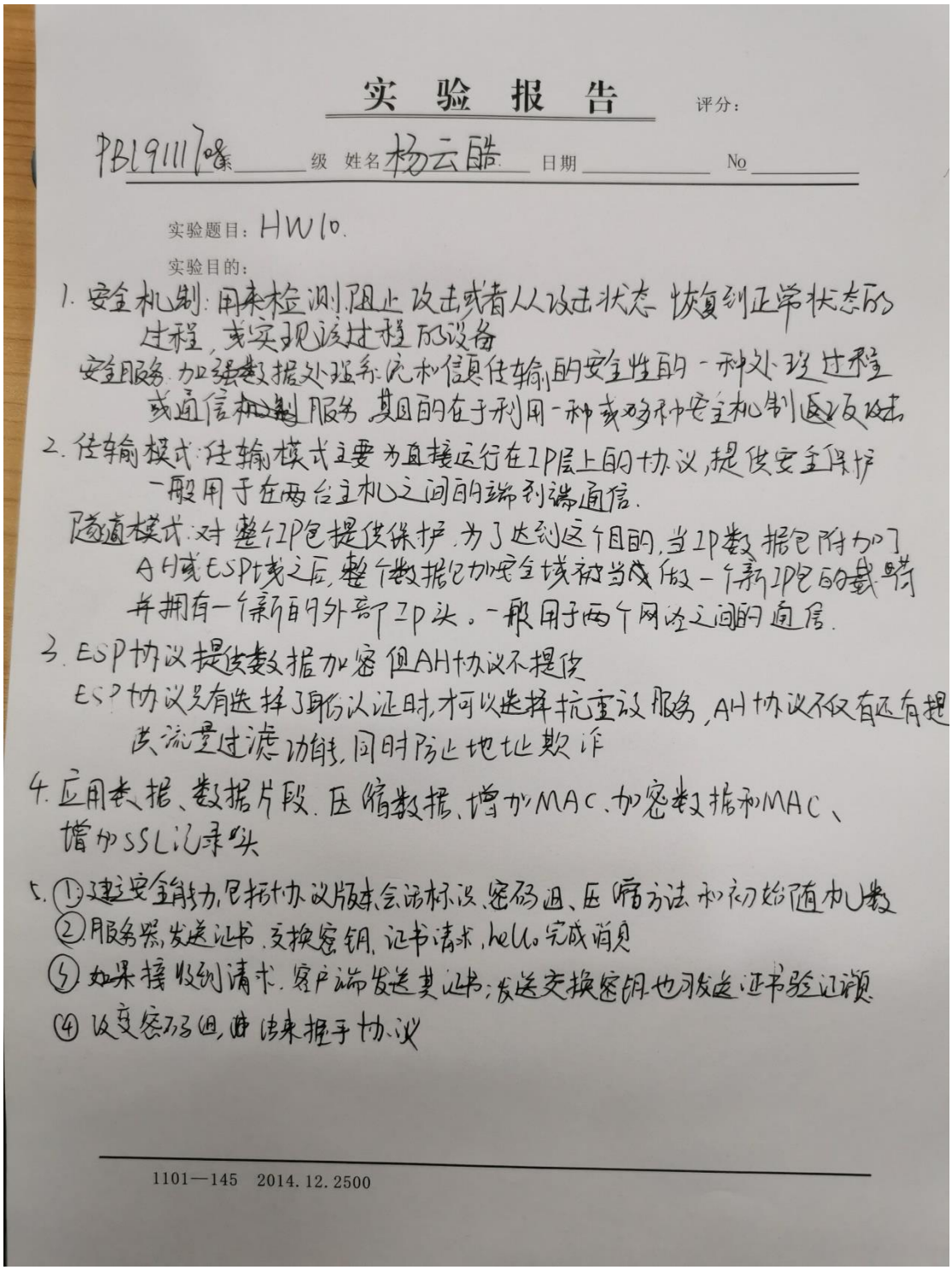
第十次作业

PB19111708 杨云皓



实 验 报 告 评分：

PB19111708 级 姓名 杨云皓 日期 No

实验题目：HW10.

实验目的：

1. 安全机制：用来检测、阻止攻击或者人从攻击状态恢复到正常状态的过程，或实现该过程的设备

安全服务：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务，其目的在于利用一种或多种安全机制反攻反攻击

2. 传输模式：传输模式主要为直接运行在IP层上的协议，提供安全保护一般用于在两台主机之间的端到端通信.

隧道模式：对整个IP包提供保护，为了达到这个目的，当IP数据包附加了AH域或ESP域之后，整个数据包加安全域被当成做一个新IP包的载荷并拥有一个新的外部IP头。一般用于两个网络之间的通信.

3. ESP协议提供数据加密但AH协议不提供

ESP协议只有选择了身份认证时，才可以选择抗重放服务，AH协议不仅有还有提供流量过滤功能，同时防止地址欺诈

4. 应用表、数据片段、压缩数据、增加MAC、加密数据和MAC、增加SSL记录头

5. ①建立安全能力，包括协议版本、会话标识、密码组、压缩方法和初始随机数

②服务器发送证书、交换密钥、证书请求，hello完成消息

③如果接收到请求，客户端发送更证书；发送交换密钥也可发送证书验证消息

④改变密码组，握手协议

1101—145 2014.12.2500