网络攻击与防御 2024 秋

一、概念题

1、 CIA 是什么

2、 tcp syn fin 原理

3、 旗标抓取技术和服务指纹分析是什么

4、 口令破解防御技术

5、 ARP 欺骗原理和实施步骤

6、 同源策略的定义和不考虑同源策略的情况

7、 csrf 的原理和防御

二、简答题

1、 渗透测试七步骤 分别做什么

2、 SQL 注入步骤、防御措施

3、 拒绝服务定义;分类;防御

三、代码分析题

栈缓冲区溢出。和书上内容完全一致，最后考了个 shellcode（定义，编写步骤）

倒数第二问是至少要输入多少字符才能到返回地址

画栈帧图，传入 12345678 和 01234567 的溢出结果，原因

第一问是问代码有什么问题，出现问题的原因是什么