|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2025春《基于TCP流重组的软件行为分析》课程设计检查表** | | | | |
|  | **班级** |  | **学号** |  |
|  | **姓名** |  | **截包文件名** |  |
|  |  |  |  |  |
| **TCP**  **流重组**  **（40分）** | 客户端IP  （2分） |  | 服务器IP  （2分） |  |
| 用户名  （2分） |  | 口令  （2分） |  |
| 文件名  （2分） |  | 数据连接模式  （2分） |  |
| 数据连接监听IP（2分） |  | 数据连接监听  端口（2分） |  |
| 文件MD5  （24分） |  | | |
| **软件行为分析**  **（60分）** | **漏洞1** | | | |
| 漏洞类型  （2分） |  | 导致漏洞的函数  （2分） |  |
| 函数被调用地址  （3分） |  | | |
| 漏洞成因  （4分） |  | | |
| 触发条件  （4分） |  | | |
| **漏洞2** | | | |
| 漏洞类型  （2分） |  | 导致漏洞的函数  （2分） |  |
| 函数被调用地址  （3分） |  | | |
| 漏洞成因  （4分） |  | | |
| 触发条件  （4分） |  | | |
| **恶意代码1** | | | |
| 功能类型  （2分） |  | 使用的系统调用  （2分） |  |
| 函数被调用地址  （3分） |  | | |
| 具体功能描述  （4分） |  | | |
| 触发条件  （4分） |  | | |
| **恶意代码2** | | | |
| 功能类型  （2分） |  | 使用的系统调用  （2分） |  |
| 函数被调用地址  （3分） |  | | |
| 具体功能描述  （4分） |  | | |
| 触发条件  （4分） |  | | |
| **总分** | |  | **评分人** |  |
| 注：  ①“函数被调用地址”填写**导致漏洞发生**的16进制静态虚拟地址  ②“触发条件”填写触发漏洞或恶意代码的网络输入需满足的条件 | | | | |