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 sample2.pcapng

TCP 流重组（40 分） 以 sample2.pcapng 为例	客户端 IP（2 分）	10.0.2.7	服务器 IP（2 分）	10.0.2.8
	用户名（2 分）	seed	口令（2 分）	dees
	文件名（2 分）	cs-test.2	数据连接模式（2 分）	PASV
	数据连接监听 IP（2 分）	10.0.2.8	数据连接监听端口（2 分）	34160
	文件 MD5（24 分）	71a8c15e892f6643c6bb70ebe7fc6c97 （可在 linux 系统中执行“md5sum 文件名”命令得到）		
软件行为分析（60 分） 以 demo 程序为例	**漏洞 1**			
	漏洞类型（2 分）	栈溢出 （按指导手册 3.2 节的四级标题）	导致漏洞的函数（2 分）	strcpy
	函数被调用地址（3 分）	0x1435 （如果存在多个，需要写函数名称和顺序，例如 DF 漏洞需要写：“第一次 free 函数地址：0xABCD；第二次 free 地址：0xCDEF”）		
	漏洞成因（4 分）	使用 strcpy 字符拷贝时，没有做边界检查（或拷贝长度检查），目标数组大小只有 14B 但拷贝数据大小可以最多为 100B （原因概述 2 分，例如没有进行边界或者长度检查；具体情况占分，例如源数据长度、目的缓存大小。每种漏洞需要描述的原因见指导手册）		
	触发条件（4 分）	输入的第 2 个元素为字符 A（或 65）且第 3 个元素为字符 B（或 66） （所有条件一共 4 分，不会出现 4 个以上条件，验收样本一般为 2 个条件各 2 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）	开启后门 （按指导手册 3.2 节的四级标题）	使用的系统调用 （2 分）	system （使用多个系统调用完成一个恶意代码功能时用逗号分隔）
	函数被调用地址 （3 分）	0x13D7 （如果是多个函数，依次列出函数名和调用地址，例如：“函数名 1：0xABCD，函数名 2：0xCDEF”，一般不会超过 3 个函数）		
	具体功能描述 （4 分）	利用 system 函数调用 NC 指令创建额外监听端口，端口号为 54321 （概述 2 分，说明主要功能，例如创建额外端口；具体行为描述 2 分，例如端口号等信息。每种恶意代码需要描述的信息见指导手册）		
	触发条件 （4 分）	输入的第 9 个元素为字符 X（或 88） （所有条件一共 4 分，不会出现 4 个以上条件，验收样本一般为 2 个条件各 2 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