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 pkt593750.pcapng

TCP 流重组（40 分）	客户端 IP（2 分）	172.16.5.200	服务器 IP（2 分）	172.16.5.1
	用户名（2 分）	wyc	口令（2 分）	cyw
	传输文件名（2 分）	test2	文件数据连接模式（2 分）	PASV
	文件数据连接监听 IP（2 分）	172.16.5.1	文件数据连接监听端口（2 分）	45517
	文件 MD5（24 分）	f0fb47409d8353ae8c07ad6858a1dac5		
软件行为分析（60 分）	**漏洞 1**			
	漏洞类型（2 分）	栈溢出	导致漏洞的函数（2 分）	memcpy
	函数被调用地址（3 分）	0x15AA，0x15DA		
	漏洞成因（4 分）	使用 memcpy 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 6B 但拷贝数据大小可以很大，导致覆盖栈空间。		
	触发条件（4 分）	在 main 函数中，输入数据最终存储至 dest 数组，内容需包含 MyfateisminenotHeaven's!，且 dest[11] 与 dest[23] 的最小公倍数为 80，才会调用漏洞函数 threemonkey。当 dest[12] == 85 时，触发第一次 memcpy，目标数组大小 6B，拷贝数据最高为 10B，导致栈溢出。当 dest[15] == 73 时，触发第二次 memcpy，目标数组大小 6B，拷贝数据大小由 dest[22] 控制，可覆盖栈上任意数据。		
	漏洞 2			
	漏洞类型（2 分）	UAF	导致漏洞的函数（2 分）	free
	函数被调用地址（3 分）	free 函数在 0x1544 被调用，use 在 0X1566		
	漏洞成因（4 分）	在使用 free 函数释放内存时，未将 ptr 指针置空或解引用，导致指针仍指向已释放的内存区域（即悬空指针）。随后，程序利用该指针写入数据，ptr[1] =		

		result，会造成程序崩溃，触发 Use After Free（UAF）漏洞。此漏洞可能导致程序崩溃、数据损坏，或被攻击者利用执行恶意代码。具体而言，dest[9] <= 48 时，调用 free 释放内存，但指针未被清空；当 dest[30] == 102 时，程序通过该悬空指针向已释放的内存写入数据。		
	触发条件（4 分）	按照前述栈溢出漏洞的触发条件（dest 数组包含 MyfateisminenotHeaven's!，dest[11] 与 dest[23] 的最小公倍数为 80），触发 threemonkey 函数。随后，利用栈溢出漏洞将 v3 的值覆盖为 77，以调用漏洞函数 wuzhishan。当 dest[9] <= 48 时，触发 free 函数释放内存；当 dest[30] == 102 时，触发 use 写入数据。		
	恶意代码 1			
	功能类型（2 分）	开启后门	使用的系统调用（2 分）	system
	函数被调用地址（3 分）	0x14B7		
	具体功能描述（4 分）	执行 system("nc -l -p 54321") ，其中-l 开启监听，-p 指定端口，该命令会启动 Netcat（nc）监听服务，绑定到本地 TCP 54321 端口，等待外部连接。		
	触发条件（4 分）	运行程序会在 12345 开启监听，向该端口发送的数据会被存储至 dest 数组，数组内容需包含 MyfateisminenotHeaven's!，且同时满足 dest[3] == 83、dest[4] == 79、dest[5] == 83，然后会调用 twosandy()函数，执行恶意代码。		
	恶意代码 2			
	功能类型（2 分）	系统文件删除与修改	使用的系统调用（2 分）	调用 remove 函数,底层系统调用的是 unlink()
	函数被调用地址（3 分）	0x1468		
	具体功能描述（4 分）	调用 remove 函数，利用 unlink 系统调用删除 /etc/passwd 文件。unlink 函数以文件路径 /etc/passwd 作为参数，执行时会从文件系统中移除该文件，导致系统用户账户信息丢失，可能破坏系统认证机制。		
	触发条件（4 分）	运行程序会在 12345 开启监听，向该端口发送的数据会被存储至 dest 数组，数组内容需包含 MyfateisminenotHeaven's!，且满足 (dest[1] & (dest[2] == 119)) != 0，然后会调用 onepigsy() 函数，执行恶意代码。		
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