作业提交，以“班级\_学号\_姓名”的方式命名，如：网安2104\_U202112131\_邬雪菲

1. 调研并阐述xz-utils 后门的利用原理。

通过供应链攻击的方式劫持sshd服务的身份认证逻辑，从而绕过ssh身份认证并发送任意代码执行，最终实现远程代码执行攻击（RCE）。

具体来说，首先在liblzma库中植入后门代码，因某些Linux发行版中openssh-server依赖于libsystemd0，而libsystemd0又依赖于liblzma5。因此，当sshd服务启动时，它会间接加载包含后门的liblzma5.so库。后门代码中将sshd服务中的公钥签名验证函数RSA\_public\_decrypt()替换，从而可以绕过sshd的身份认证，向目标系统远程发送任意代码执行。

2. 阐述如何利用漏洞程序中对printf的错误使用，实现对程序控制流的劫持？

由于printf使用格式画字符串来确定如何解释和显示参数，存在格式化字符串漏洞，如果漏洞程序提供输入不受信任的字符串作为参数的机会，则可以精心构造输入泄露内存信息，修改内存值并实现控制流劫持。

具体来说，通过格式化字符串漏洞，可以覆盖栈上的返回地址，将程序重定向到内存中的任意位置，可以是攻击者写入的shellcode，或者是利用程序原有gadget构造的payload。

3. 阐述如何通过内存泄漏的方式，对ASLR防御进行绕过？

可以通过Got表泄露函数地址，由于已知版本的libc库函数相对地址是固定的，由泄露的函数真实地址可以计算出libc基地址，从而可以定位libc库函数，并发送payload劫持程序控制流，利用libc库的提权函数等关键代码获取系统控制，即实施Ret2Libc或ROP攻击。

1. 阐述使用Ret2libc方法中多函数调用，分别对32位和64位漏洞程序进行控制流劫持的原理，及其区别。

Ret2libc利用程序的栈溢出漏洞来覆盖返回地址，使其指向libc库中的代码片段（即有用的gadgets，可，然后通过多次调用这些函数来执行所需的操作。32位和64位漏洞程序的区别主要是在于函数调用的参数传递方式不同，32位linux完全通过栈来传递参数，但64位linux函数调用前六个参数是使用rdi, rsi, rdx, rcs, r8, r9 传递的，由于不是使用栈，所以构建栈上的ROP时，需要按顺序构造，把要泄漏的地址func\_got\_addr放入rdi寄存器中。

5. 解释为什么普通用户可以利用Set-UID程序对特权文件进行修改？

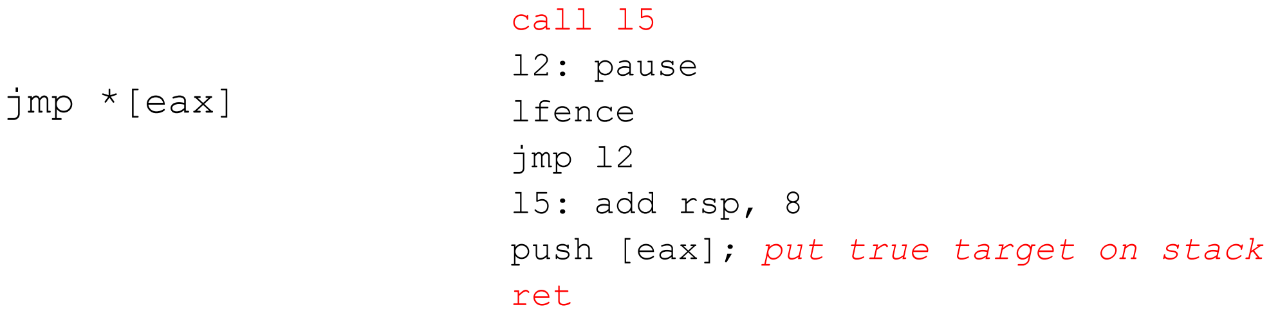
Set-UID（设置用户ID）是一种UNIX和类UNIX操作系统中的安全特性，当一个文件被设置了Set-UID位时，任何用户执行该程序都会以该文件所有者的权限来运行。所以普通用户使用set-uid程序可以获取特权级权限，由此修改特权文件。

6. 分别阐述 Prime+Probe 和 Flush+Reload两种Cache侧信道攻击方法的原理。

Prime+Probe攻击是一种利用CPU缓存一致性机制的侧信道攻击技术。在这种攻击中，攻击者首先（Prime阶段）使目标数据进入CPU的缓存。随后，攻击者探测（Probe阶段）缓存中的数据是否被访问，这通常通过监测缓存命中或未命中的延迟差异来实现。如果目标数据在缓存中被访问，那么CPU处理攻击者指令时会表现出不同的延迟模式，因为缓存一致性机制会确保数据在所有核心之间同步。通过分析这些微小的延迟变化，攻击者可以推断出目标程序的执行情况，从而获取敏感信息。

Flush+Reload攻击是另一种基于缓存的侧信道攻击技术。在这种攻击中，攻击者首先（Flush阶段）清空CPU缓存中所有数据，确保目标数据不在缓存中。然后，攻击者加载（Reload阶段）他们自己的数据到缓存中，并监测缓存的行为。如果目标程序随后访问了某些数据，CPU的缓存一致性机制将导致攻击者加载到缓存中的数据被替换出去，这可以通过监测缓存未命中事件来检测。通过分析缓存未命中的模式，攻击者可以推断出目标程序访问了哪些数据，这可能揭示出密码、密钥或其他敏感信息。

7. 下图是一种Spectre的防御方法，请解释其原理。



Spectre攻击利用了现代处理器中的推测执行（Speculative Execution）特性，通过侧信道攻击获取信息。

上述防御过程调整栈指针后，将eax寄存器指向的真实目标地址压入栈中，然后pause检查中断，ifence指令设置同步屏障。代码通过中断和混淆正常的推测执行流程，陷入循环，不去执行预测分支，使得攻击者难以利用预测分支来执行侧信道攻击。