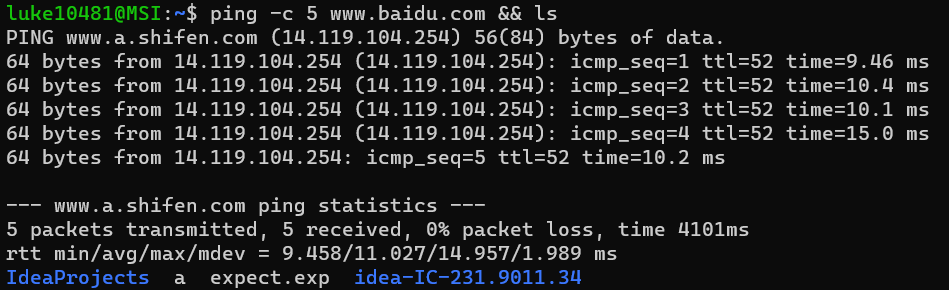
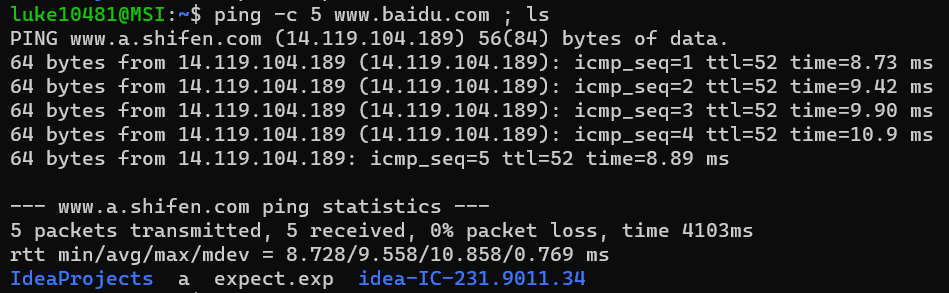
使用&&符号拼接



使用;符号拼接



使用|拼接



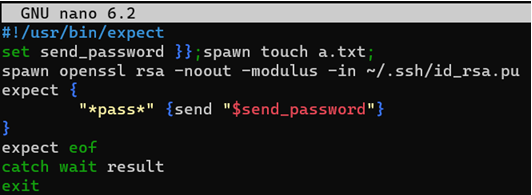
Expect spawn

当前目录文件夹情况



编辑expect.exp文件

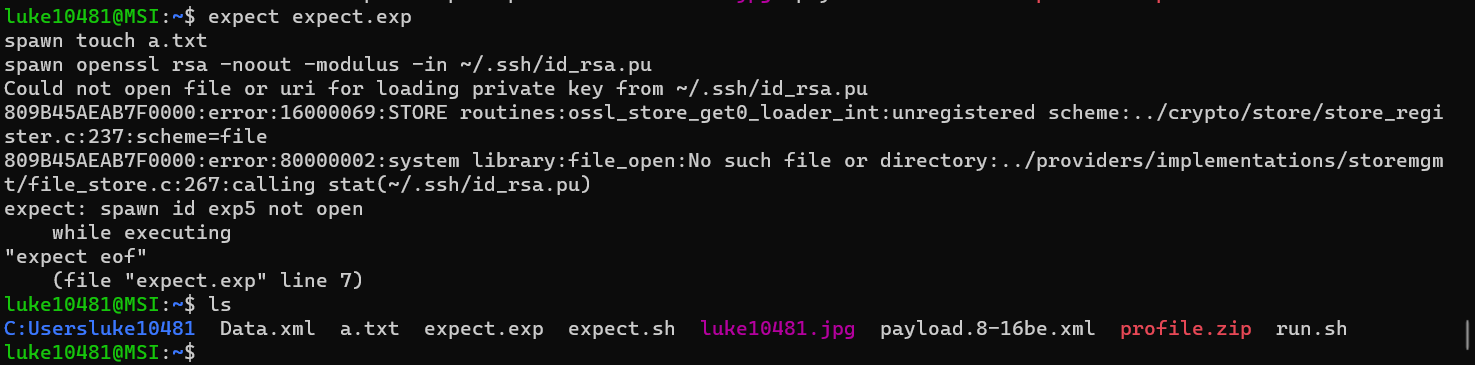
Send\_password是外部可控变量，为这个变量赋值为}};spawn touch a.txt，填充到”\*pass\*” {send “$send\_password”}的￥$send\_password里面，因为spawn openssl rsa -noout -modulus -in ~/.ssh/is\_rsa.pu执行失败，不需要针对对”符号进行闭合



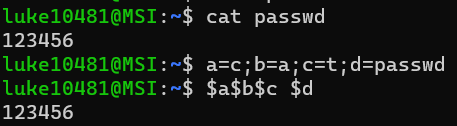
执行该expect.exp文件



发现当前文件目录多了a.txt，证明touch a.txt成功执行，成功命令注入



针对字符限制的绕过，将字符拆开abcd分别赋值，再通过$分别组合字符，构造命令注入



针对空格的限制绕过，用<>代替空格字符



绕过字符长度限制，若限制只能输入5个字符，通过\字符分段输入命令cat expect.exp，成功执行命令

