某局点堡垒机SFTP访问linux主机失败的经验案例

运维审计 姜霁琛 2021-12-10 发表

组网及说明

无

问题描述

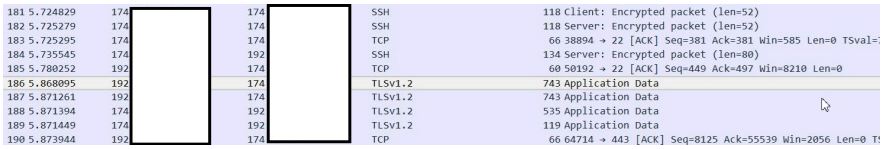
现场纳管linux主机资产，通过ssh访问该主机正常，但sftp方式访问时报错：获取远程目录名出错

过程分析

在内网测试不经过堡垒机访问sftp正常，也能传输文件；直接让现场sftp堡垒机地址测试是一样的报错。

测试帐号未托管，使用any类型的账号，手动输入用户名密码

在堡垒机上使用tcpdump工具抓包，发现能够看到正常交互的ssh报文



181	5.724829	174	174	SSH	118 Client: Encrypted packet (len=52)
182	5.725279	174	174	SSH	118 Server: Encrypted packet (len=52)
183	5.725295	174	174	TCP	66 38894 → 22 [ACK] Seq=381 Ack=381 Win=585 Len=0 TSval=
184	5.735545	174	192	SSH	134 Server: Encrypted packet (len=80)
185	5.780252	192	174	TCP	60 50192 → 22 [ACK] Seq=449 Ack=497 Win=8210 Len=0
186	5.868095	192	174	TLSv1.2	743 Application Data
187	5.871261	192	174	TLSv1.2	743 Application Data
188	5.871394	174	192	TLSv1.2	535 Application Data
189	5.871449	174	192	TLSv1.2	119 Application Data
190	5.873944	192	174	TCP	66 64714 → 443 [ACK] Seq=8125 Ack=55539 Win=2056 Len=0 T

进一步测试发现，不经过堡垒机访问sftp服务时，连接需要40s，但是查看堡垒机的连接超时默认要求为20s

交互超时时间	运维审计系统对设备进行登录或执行命令等交互操作的超时时间。单位为秒，范围为0~9999秒。缺省值为20秒。 仅影响字符会话、自动化脚本、帐号改密。 **Note:** 交互超时时间必须小于任务执行超时时间。

解决方法

回溯现场的linux主机，发现近期做过安全加固操作，因此对于登陆的用户名有安全性要求，通过堡垒机登陆的用户名为 newroot，由于安全加固的原因，连接时间变成了40s，超过了堡垒机的交互超时时间20s，因此出现登陆失败的情况。将用户名改为安全加固要求的root后，能正常通过堡垒机sftp到主机。

经验学习：通过堡垒机访问失败，不单单仅要排查堡垒机的问题，如果确定堡垒机的配置无问题，抓包也都有报文交互时，也要建议现场排查一下内网的服务器是否有问题。