9 堡垒机【内网运维审计平台】

堡垒机：安全管理平台转

0x01 实验环境

Jumpserver

下载地址：https://github.com/jumpserver/jumpserver

0x02 原理介绍

1)原理

■ 部署于核心，旁路

■内部的人员通过这个设备，访问我们的内部各种网络、服务器、中间件、安全设备等。

■SSH TELNET 3389

2) 功能

核心功能列表

身份认证 Authentication	登录认证	资源统一登录与认证
		LDAP/AD 认证
		RADIUS 认证
		OpenID 认证（实现单点登录）
	MFA认证	MFA 二次认证（Google Authenticator）
		RADIUS 二次认证
	登录复核（X-PACK）	用户登录行为受管理员的监管与控制
账号管理 Account	集中账号	管理用户管理
		系统用户管理
	统一密码	资产密码托管
		自动生成密码
		自动推送密码
		密码过期设置
	批量改密（X-PACK）	定期批量改密
		多种密码策略
	多云纳管（X-PACK）	对私有云、公有云资产自动统一纳管
	收集用户（X-PACK）	自定义任务定期收集主机用户
	密码匣子（X-PACK）	统一对资产主机的用户密码进行查看、更新、测试操作
授权控制 Authorization	多维授权	对用户、用户组、资产、资产节点、应用以及系统用户进行授权
		资产以树状结构进行展示
	多维授权	对用户、用户组、资产、资产节点、应用以及系统用户进行授权
	资产授权	资产以树状结构进行展示
		资产和节点均可灵活授权
		节点内资产自动继承授权
		子节点自动继承父节点授权
	应用授权	实现更细粒度的应用级授权
		MySQL 数据库应用、RemoteApp 远程应用（X-PACK）
	动作授权	实现对授权资产的文件上传、下载以及连接动作的控制
	时间授权	实现对授权资源使用时间段的限制
	特权指令	实现对特权指令的使用（支持黑白名单）
	命令过滤	实现对授权系统用户所执行的命令进行控制
	文件传输	SFTP 文件上传/下载
	文件管理	实现 Web SFTP 文件管理
	工单管理（X-PACK）	支持对用户登录请求行为进行控制
	组织管理（X-PACK）	实现多租户管理与权限隔离

安全审计 Audit	操作审计	用户操作行为审计
	会话审计	在线会话内容审计
		历史会话内容审计
	录像审计	支持对 Linux、Windows 等资产操作的录像进行回放审计
		支持对 RemoteApp（X-PACK）、MySQL 等应用操作的录像进行回放审计
	指令审计	支持对资产和应用等操作的命令进行审计
	文件传输	可对文件的上传、下载记录进行审计

0x03 实践操作