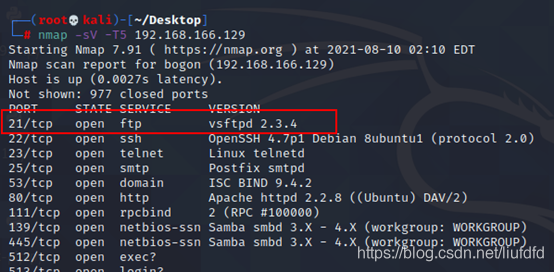
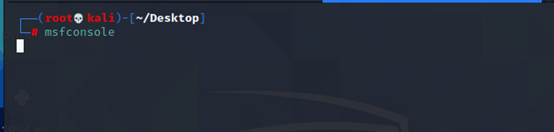
**metasploitable2靶机**

通过nmap扫描查找到vsftpd2.3.4开启

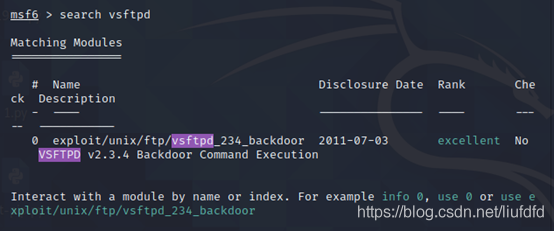


攻击

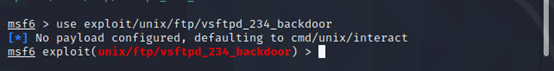
使用msfconsole工具 调出metasploit



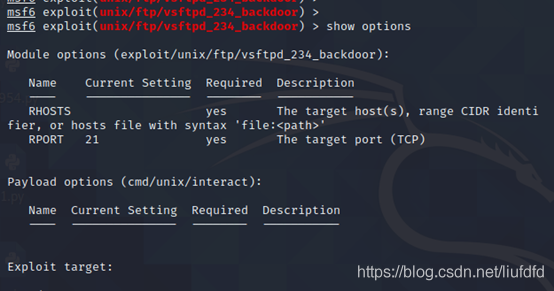
使用search 查找模块



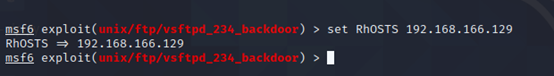
使用use设置模块



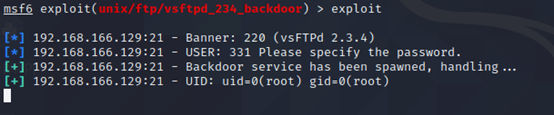
使用show options查看需配置的参数



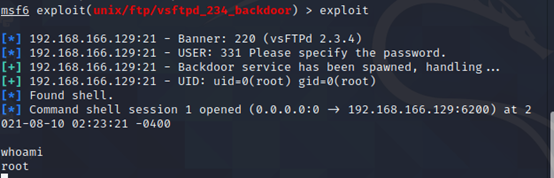
使用set设置需配置的参数



使用exploit进行攻击



攻击成功获取到靶机的权限



**22，23，3306，5432，5900 端口 弱密码**

可以使用爆破出账号密码

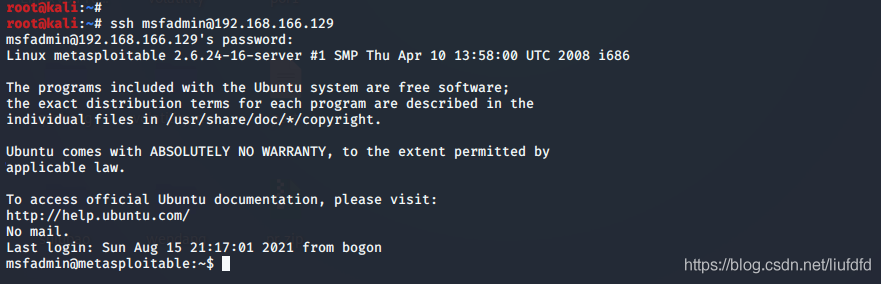
系统或者数据库的登录用户，密码简单或者和用户名相同，容易通过暴力破解手段来获取密码。  
所有使用用户名/密码登录的系统/软件都有可能存在此问题。

**在Metasploitable2中，系统口令、MySQL、PostgresQL和VNC远程登录都存在弱密码漏洞**

系统弱密码登录

Ssh

账号msfadmin密码msfadmin



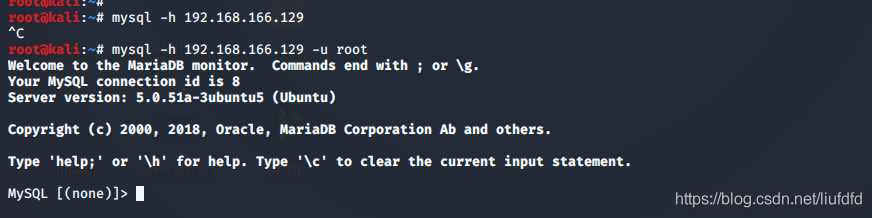
telnet

账号msfadmin密码msfadmin进行登录



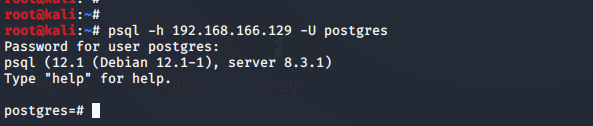
Mysql

账号root  密码为空



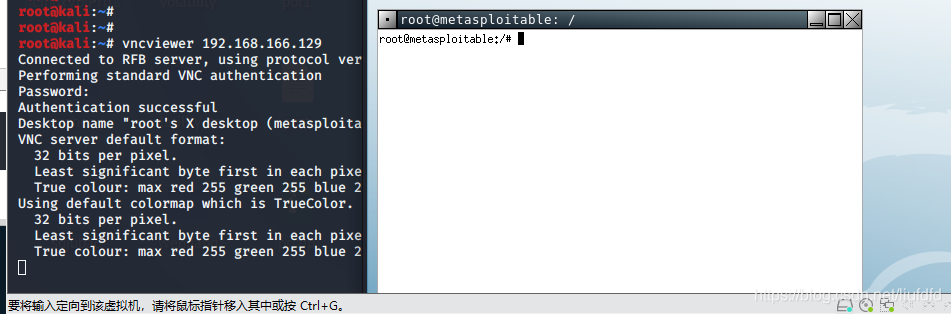
Postgresql

账号portgres密码 postgres



Vnc

密码passwoord



**139端口 445端口  smbd 3.X - 4.X**

Samba 中负责在 SAM 数据库更新用户口令的代码未经过滤便将用户输入传输给了  
/bin/sh  
如果在调用 smb.conf 中定义的外部脚本时，通过对 /bin/sh 的MS-RPC调用提交了恶意输入的话，就可能允许攻击者以 nobody 用户的权限执行任意命令。

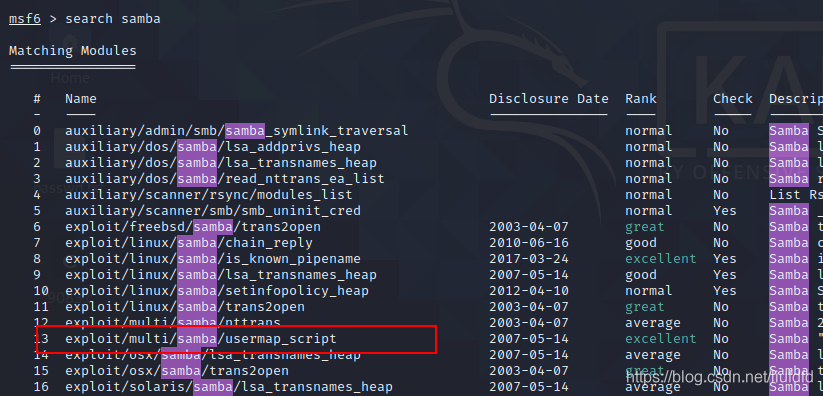
使用nmap扫描



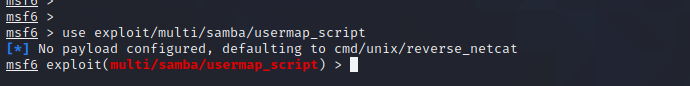
使用msfconsole工具



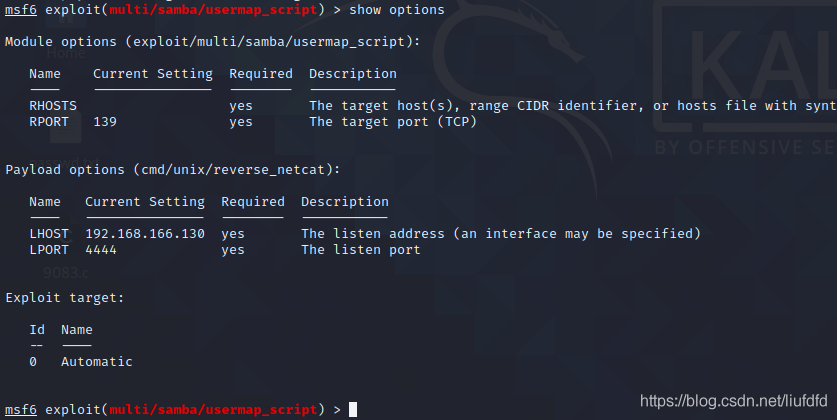
使用search查找模块



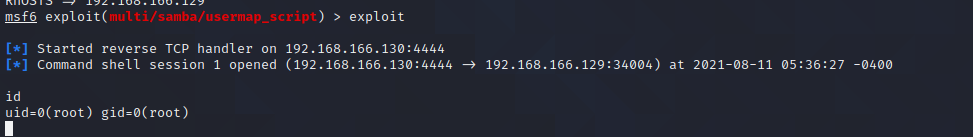
使用use设置模块



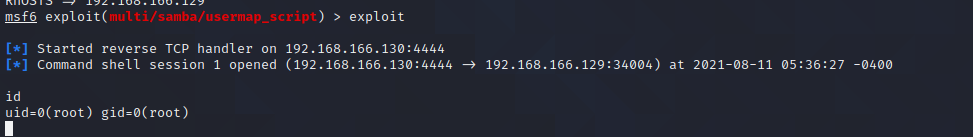
使用show option查看需配置的参数



使用set设置参数



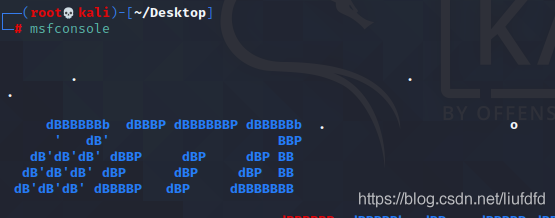
使用exploit进行攻击，攻击成功获取到权限



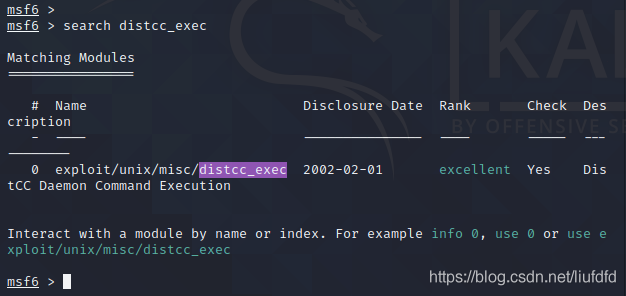
**512端口 exec**

Distcc 用于大量代码在网络服务器上的分布式编译，但是如果配置不严格，容易被滥用执行命令，该漏洞是 xcode1.5 版本及其他版本的 distcc2.x 版本配置对于服务器端口的访问不限制。

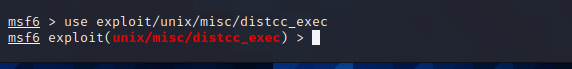
使用msfconsole工具



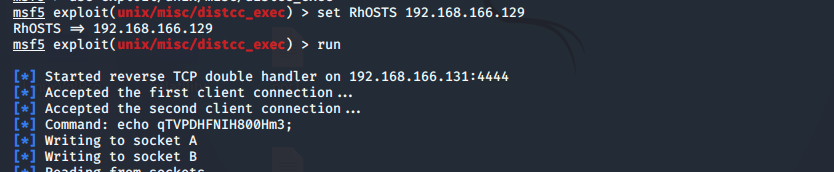
使用search命令查找模块



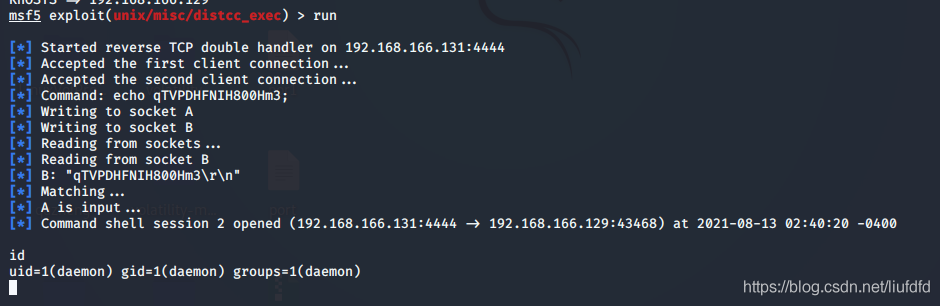
使用use设置模块



使用set设置参数



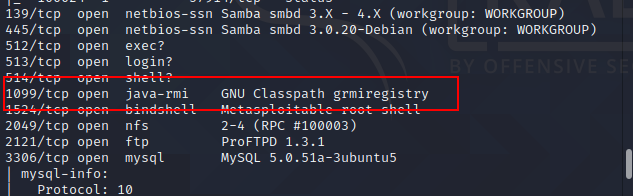
使用run进行攻击



**1099端口  Java Rmi Server命令执行漏洞**

Java RMI Serve 的 RMI 注册表和 RMI 激活服务的默认配置存在安全漏洞，可被利用导致代码执行。

使用nmap扫描发现1099端口开启



使用msfconsole工具



使用search查找模块

https://img-blog.csdnimg.cn/20210816094924909.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L2xpdWZkZmQ=,size_16,color_FFFFFF,t_70

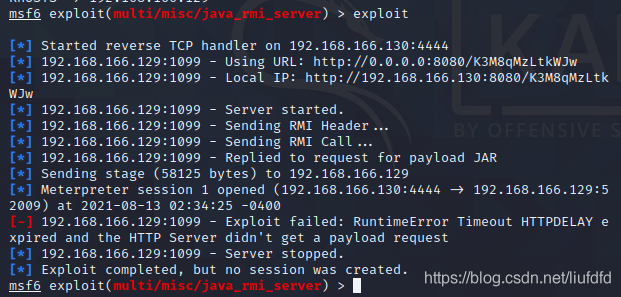
使用use设置模块

https://img-blog.csdnimg.cn/20210816094924908.png

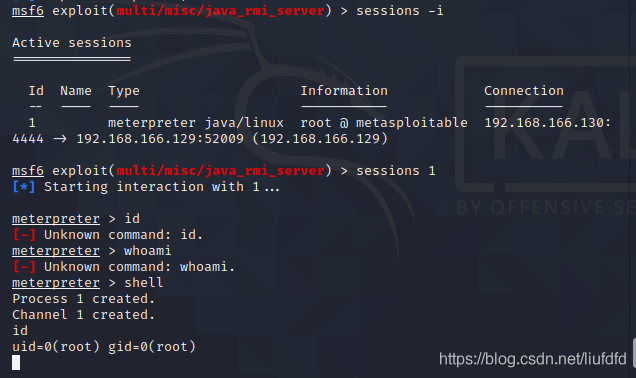
使用set设置参数

https://img-blog.csdnimg.cn/20210816094924909.png

使用exploit进行攻击



攻击成功获取到权限

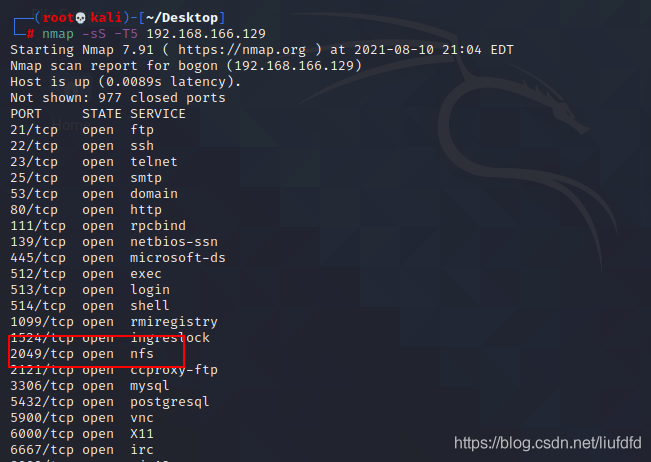


**2049，111端口 nfs**

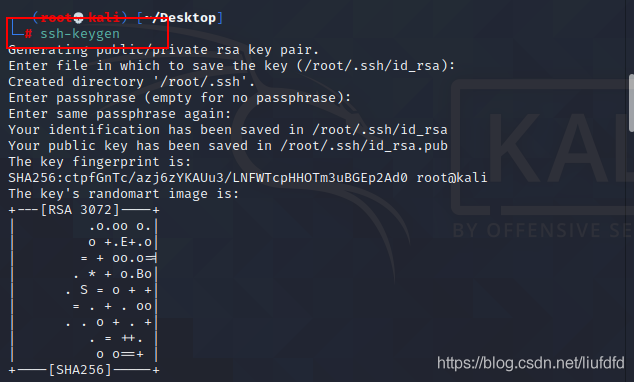
原理

NFS服务配置漏洞赋予了根目录远程可写权限，导致/root/.ssh/authorized\_keys 可被修改，实现远程ssh无密码登录

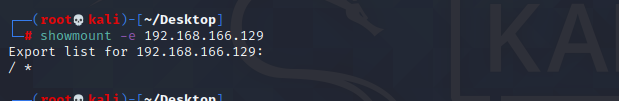
使用nmap工具查看2049端口是否开启



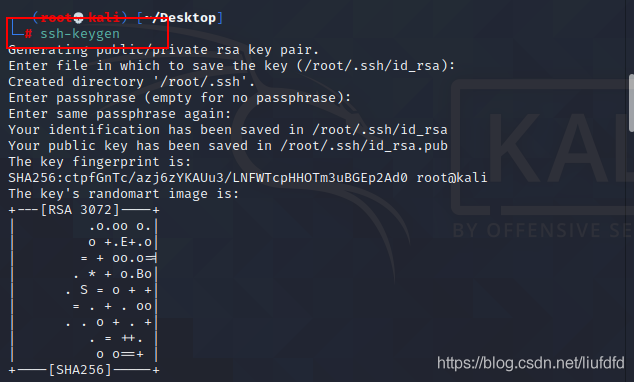
在kali上执行命令rpcinfo –p 192.168.166.129 ,查看nfs服务有无开启



使用命令showmount –e 192.168.166.129 查看其设置的远程目录列表：



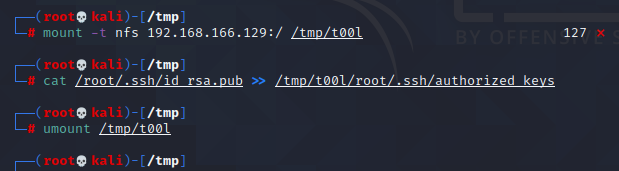
使用命令输入ssh-keygen 生成RSA公钥：



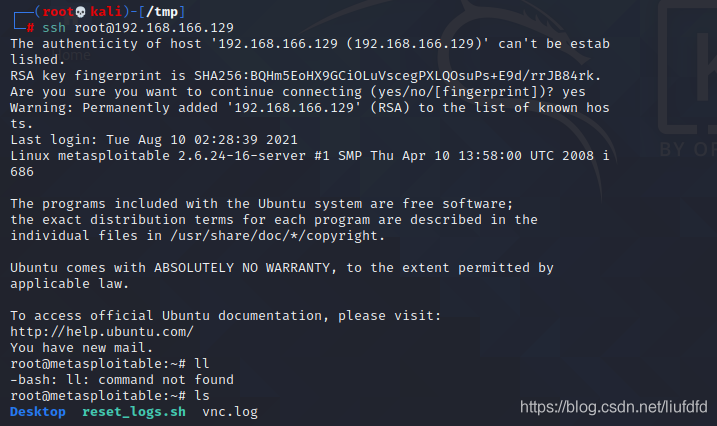
依次输入以下命令

使用命令mount –t nfs 192.168.160.129://tmp/t00l(预先创建)，把192.168.166.129的根目录挂载到/tmp/t00l/下；

cat /root/.ssh/id\_rsa.pub>>/tmp/t00l/root/.ssh/authorized\_keys，把生成的公钥追加到靶机的authorized\_keys下



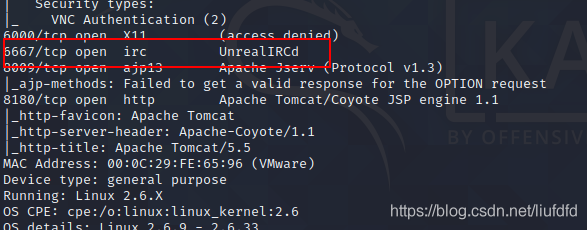
[ssh root@192.168.166.129](mailto:ssh%20root@192.168.166.129)实现无密码登录



**6667端口 UnreallRcd后门漏洞**

 DEBUG3DOLOG\_SYSTEM 宏中包含外部引入的恶意代码，远程攻击者能够执行任意代码。

使用nmap扫描发现6677端口开启



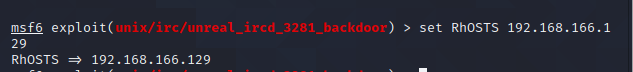
使用msfconsole工具启动metasploit



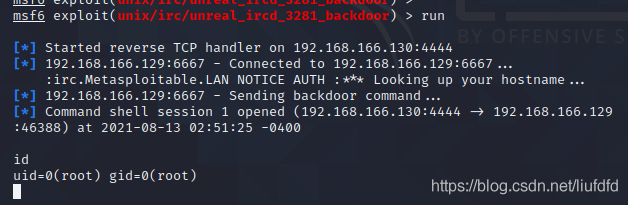
使用use设置模块

https://img-blog.csdnimg.cn/20210816095056991.png

使用set设置参数



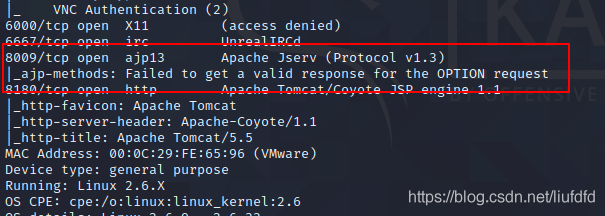
使用run进行攻击，攻击成功获取到权限



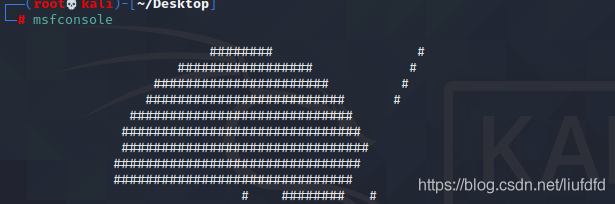
**8009端口**

GI脚本没有正确处理请求参数，导致源代码泄露，允许远程攻击者在请求参数中插入执行命令。

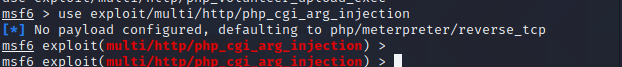
使用nmap扫描发现8009端口开启

.

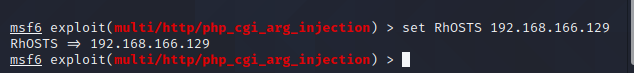
使用msfconsole命令  启动Metasploit



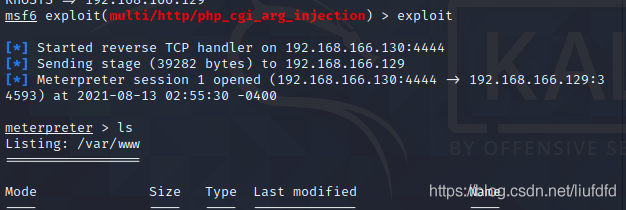
使用use设置模块



使用set设置参数



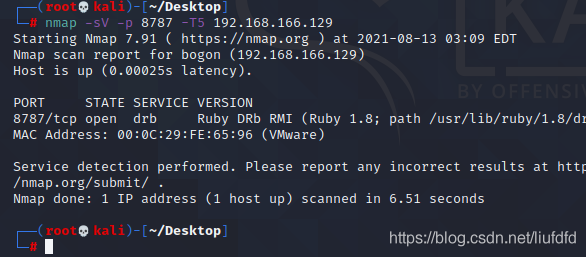
使用run进行攻击 攻击成功获取到权限



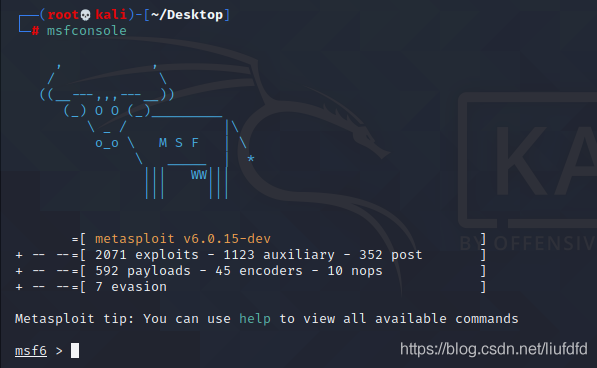
**8787端口 Ruby**

Druby配置不当，被滥用执行命令。

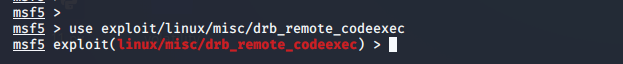
使用nmap扫描发现8787端口开启



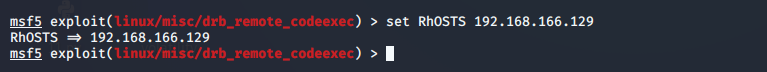
使用msfconsole 开启metasploit



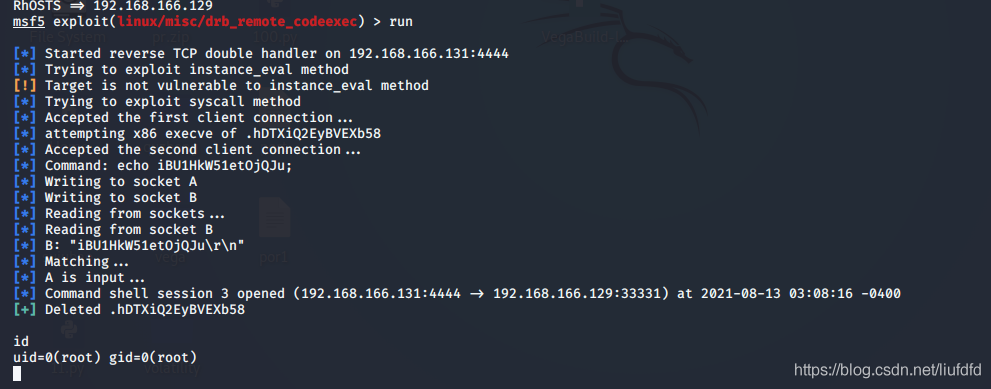
使用use设置模块



使用set设置参数



使用run进行攻击，攻击成功获取到权限

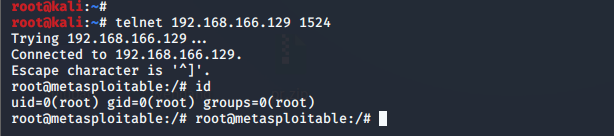


**1524 后门漏洞**

Ingreslock 后门程序监听在1524端口，连接到1524端口就可以直接获得root权限

在kali上执行 telnet 192.168.166.129 1524

直接获取到root权限



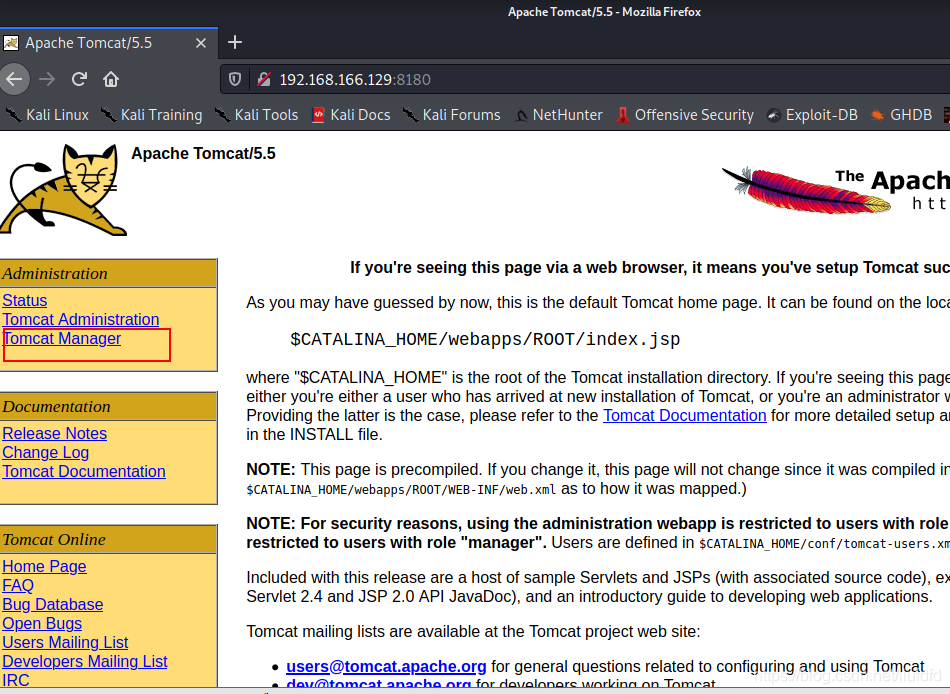
**8180端口Tomcat管理台默认口令漏洞**

**原理**

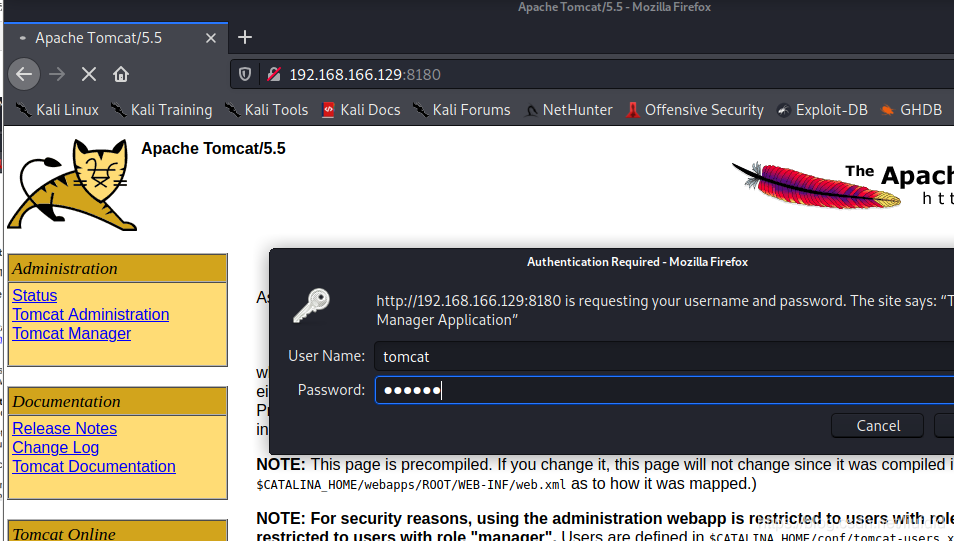
Tomcat管理台安装好后需要及时修改默认管理账户，并杜绝弱口令，成功登陆者可以部署任意web应用，包括webshell

利用步骤

使用浏览器访问8180端口



账号密码都是tomcat



**目录**