

网络攻防技术基础课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验六  MSF渗透测试 |
| 实验日期： | 2024-05-07 |
| 实验地点： | 西部片区4号楼301 |
|  | |
| 学号： | 33920212204567 |
| 姓名： | 任宇 |
| 专业年级： | 软工2021级 |
| 学年学期： | 2023-2024学年第二学期 |

1. **实验目的**

* 学习MetasploitFramework（MSF）使用。

1. **实验用到的软件或工具**

虚拟机软件：VMware Workstation Pro 17

攻击机系统：Kali

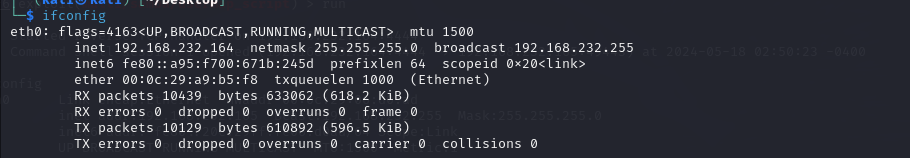
靶机系统：Metasploitable2

网络环境：两个虚拟机环境配置在同一NAT网络中

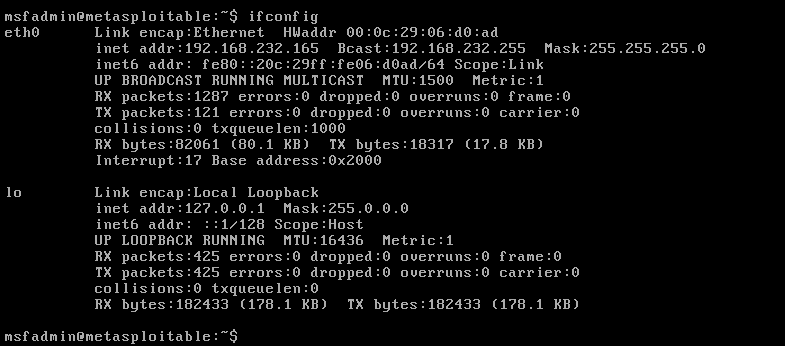
* Kali：192.168.232.164
* Metasploitable2：192.168.232.165

1. **实验过程**
2. **网络环境配置：**

攻击机：

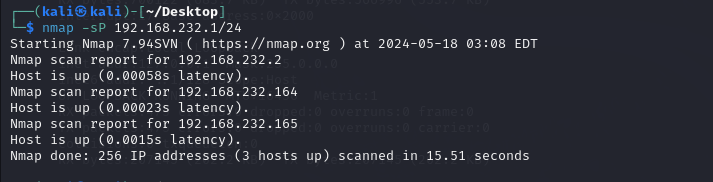


靶机：



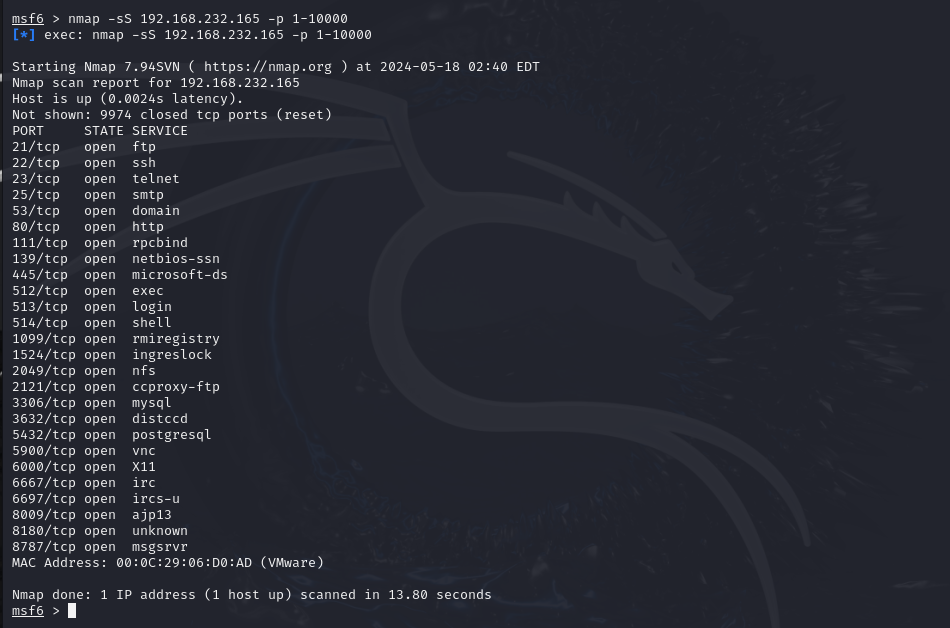
1. **前期渗透——发现主机：**

使用nmap扫描得到靶机的ip地址：

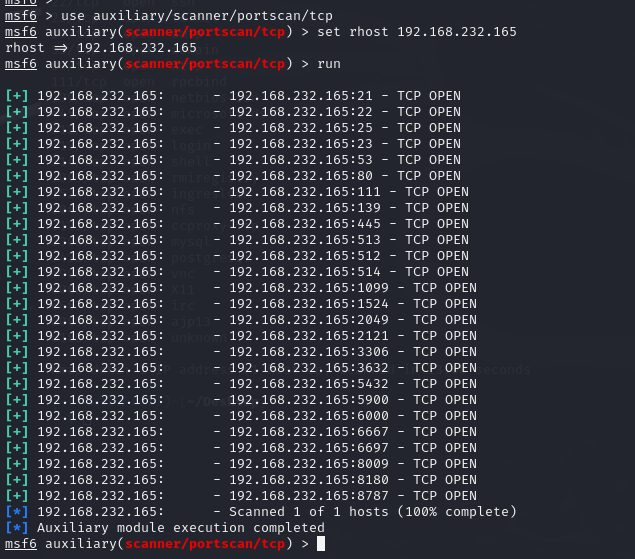


1. **前期渗透——扫描端口：**

使用nmap扫描端口：

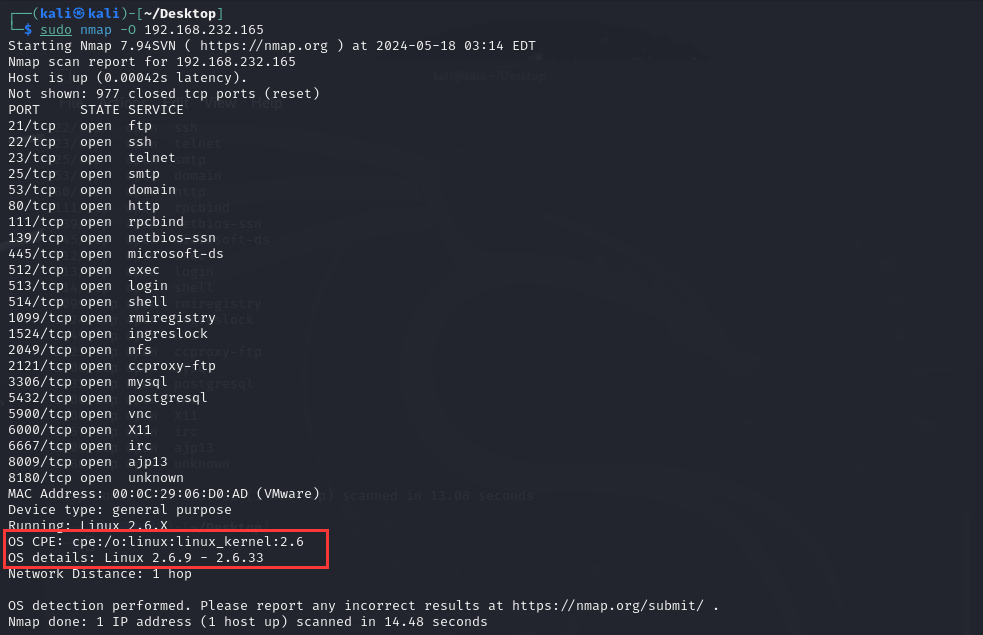


也可以使用MSF的auxiliary/scanner/portscan/tcp模块来实现：



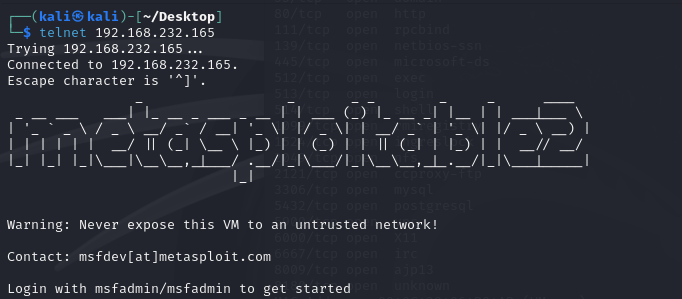
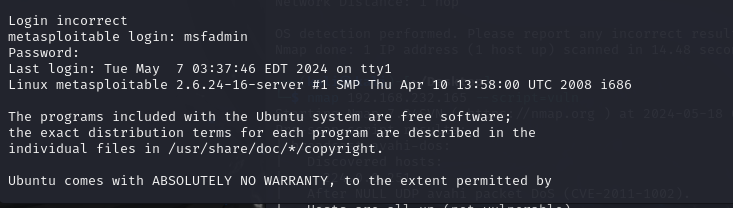
1. **前期渗透——测试漏洞：**

使用nmap -O ip 查看系统类型：



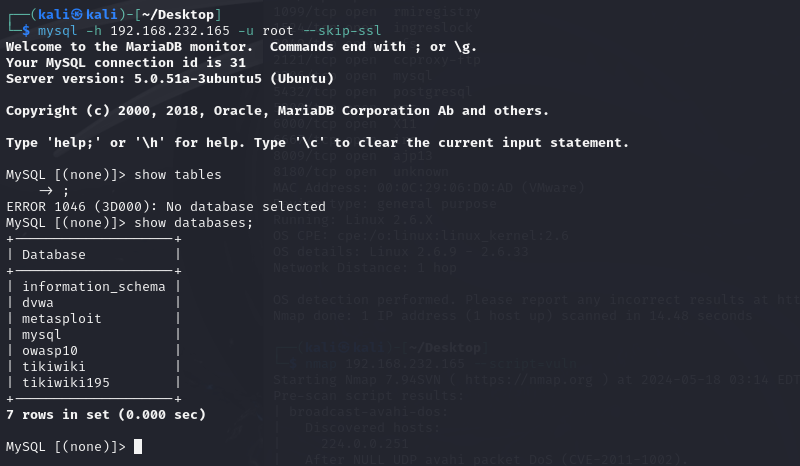
1. **弱密码漏洞——系统弱密码登录（telnet ：23端口）：**

用户名和密码都是msfadmin，可以通过telent连接：

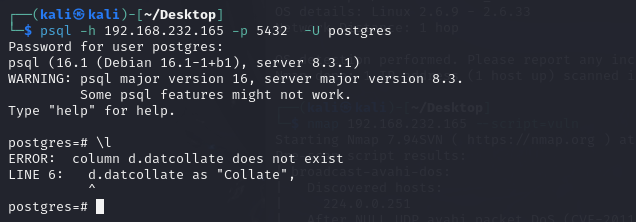
1. **弱密码漏洞——MySQL弱密码登录（端口：3306）：**

可以直接通过root账号登录到靶机上的MySQL服务：



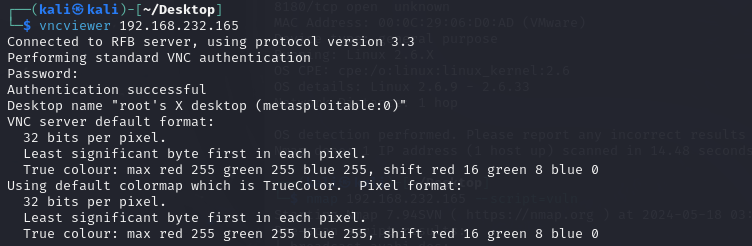
1. **弱密码漏洞——PostgreSQL弱密码登录（端口：5432）：**

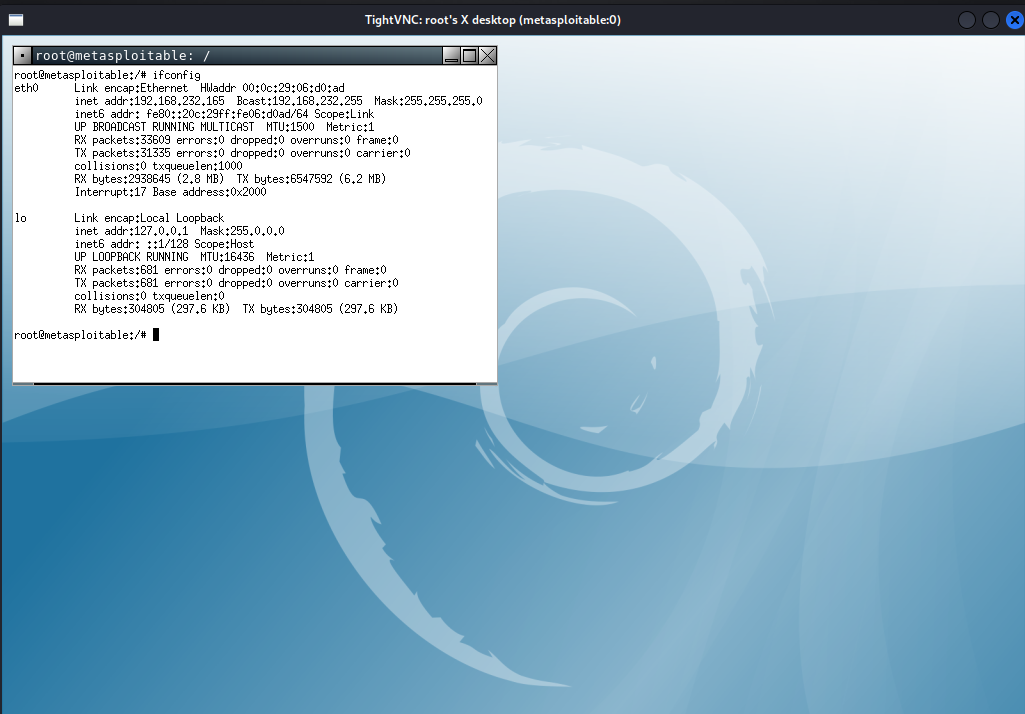
PostgreSQL会默认创建一个用户postgres，可以直接通过其登录到靶机上的PostgreSQL数据库，密码也是postgres：



1. **弱密码漏洞——VNC弱密码登录（端口：5900）：**

VNCViewer是一个远程桌面控制程序，它可以让用户通过网络连接到远程计算机并控制该计算机的桌面，密码为password。

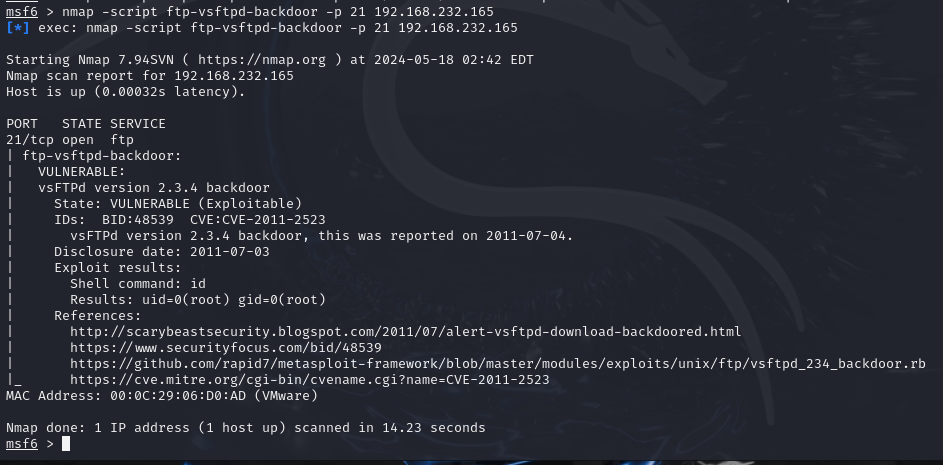




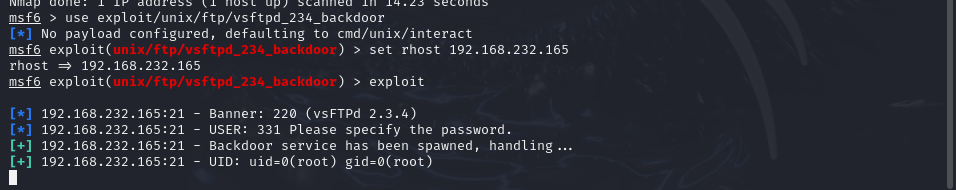
1. **Vsftpd源码包后门漏洞（21端口）：**

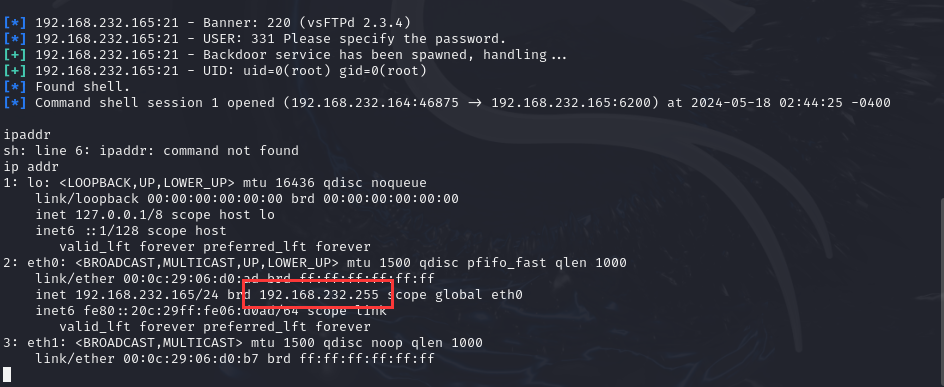
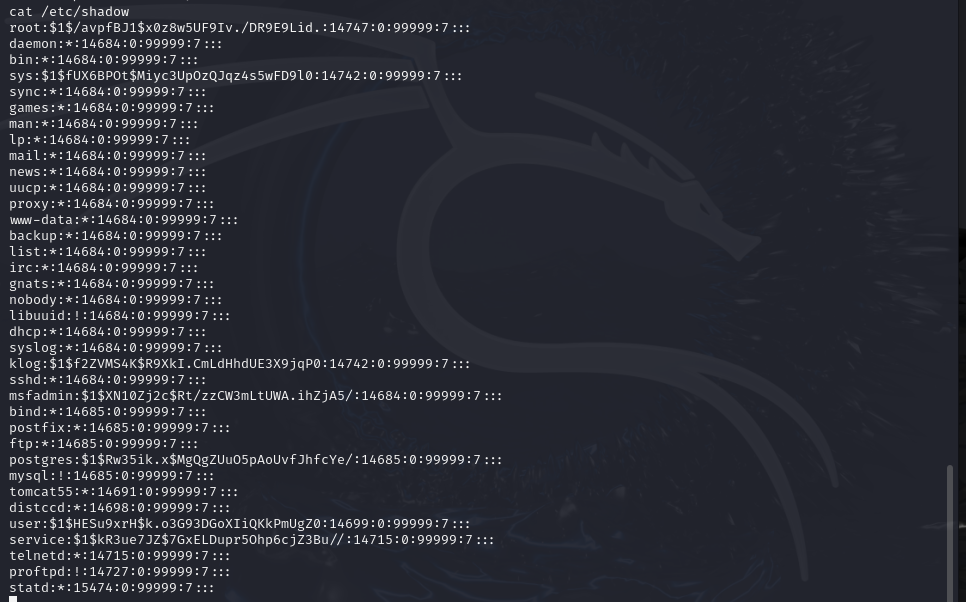
在特定版本的vsftpd服务器程序中，被人恶意植入代码，当用户名以“:)”为结尾，服务器就会在6200端口监听，并且能够执行任意代码。

首先使用nmap对应脚本进行扫描，可见靶机确实存在这个漏洞：



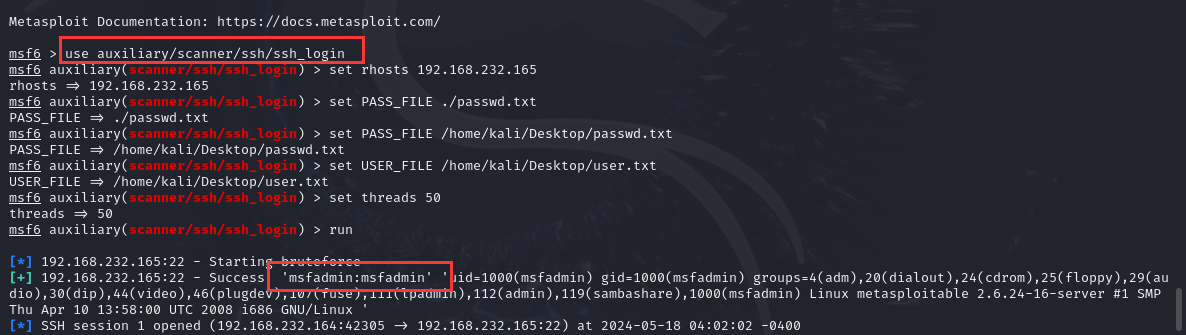
接着使用MSF中的对应模块进行渗透：



1. **SSH弱口令漏洞（22端口）:**

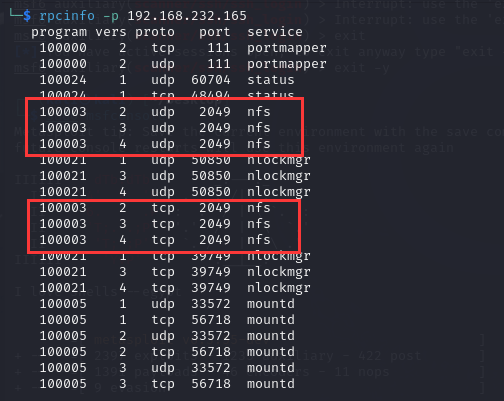
使用爆破SSH的弱口令：



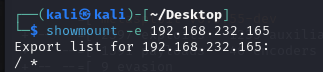
1. **Linux NFS共享目录配置漏洞（22端口）：**

NFS服务配置的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无密码登陆。

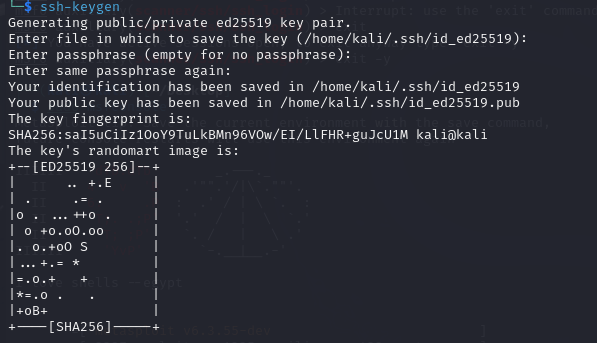
首先查看靶机上的nfs服务是否开启：



查看靶机上设置的远程共享目录列表：



生成rsa公钥命令：



在渗透机/tmp目录下新建文件夹，以备后续挂载需求：



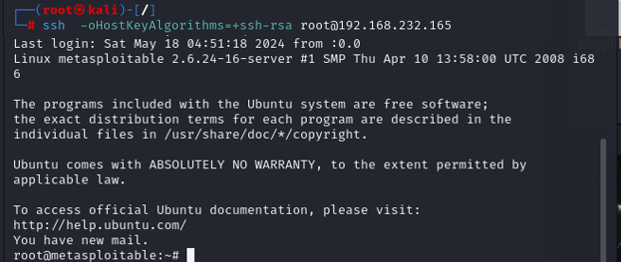
把靶机ip的根目录挂载到渗透机上新建的目录下：



把渗透机上生成的公钥追加到靶机的authorized\_keys下：



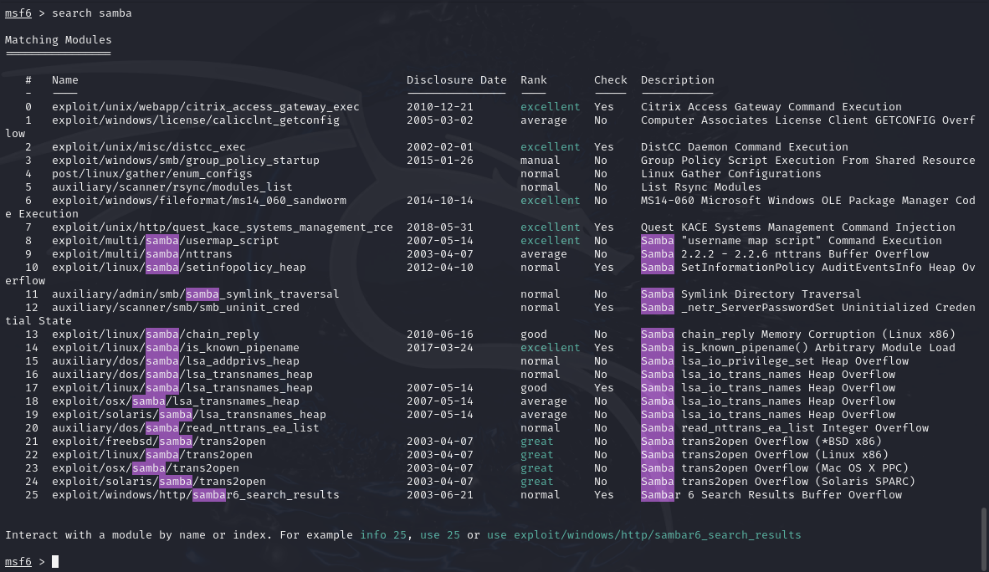
实现无密码ssh登录:



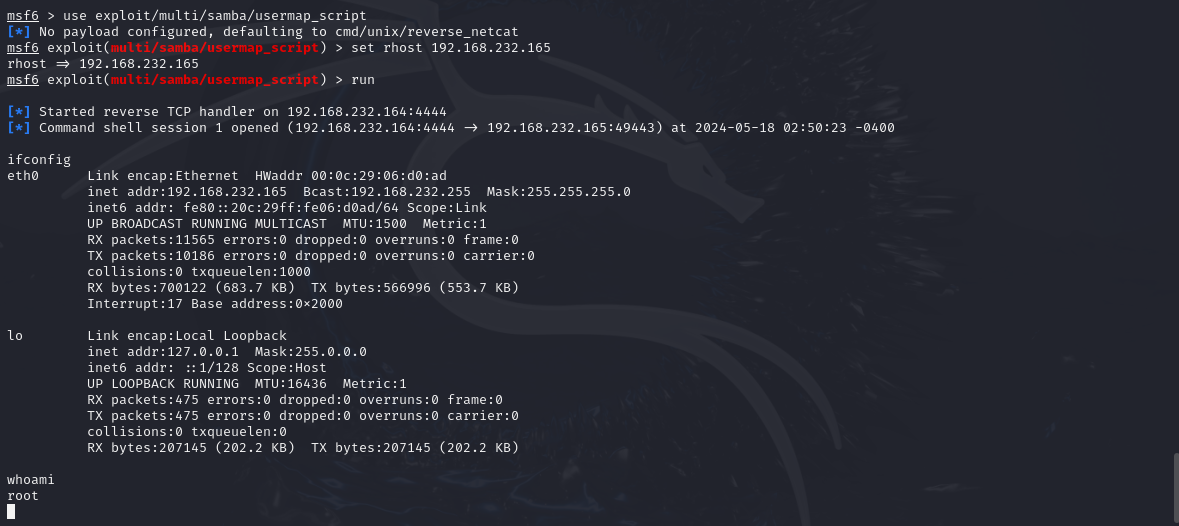
1. **SambaMS-RPC Shell命令注入漏洞（端口139）:**

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。

输入search samba ，找到针对usermap\_script安全漏洞的渗透攻击模块名称为exploirt/multi/usermap\_script：

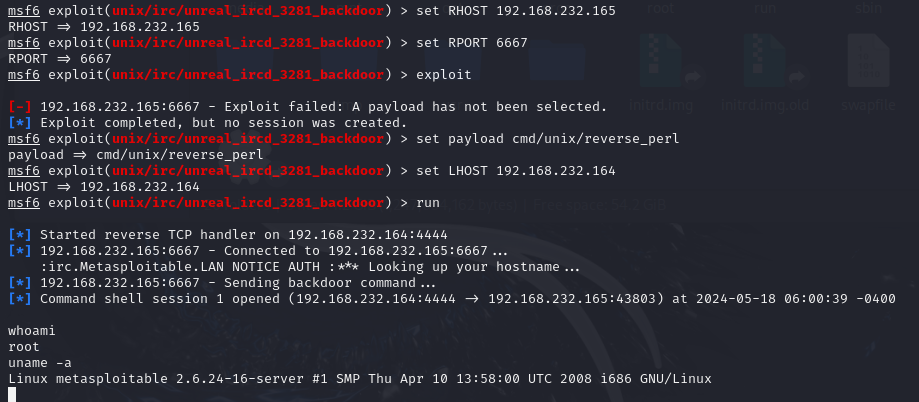


通过命令use exploit/multi/samba/usermap\_script使用渗透攻击模块，可见渗透成功后即可获得靶机的shell：：



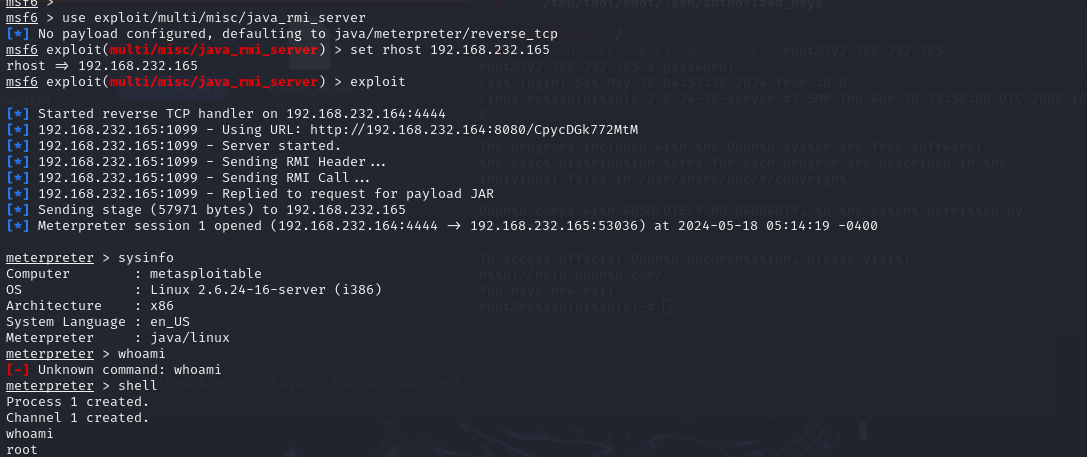
1. **UnrealIRCd后门漏洞（6667端口）:**

在2009年11月到2010年6月间分布于某些镜面站点的UnrealIRCd，DEBUG3\_DOLOG\_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。



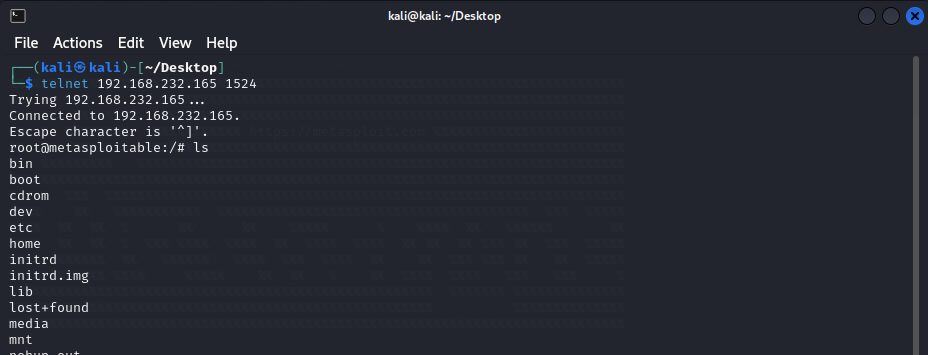
1. **Java RMI SERVER命令执行漏洞（1099端口）：**

Java RMI Server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。



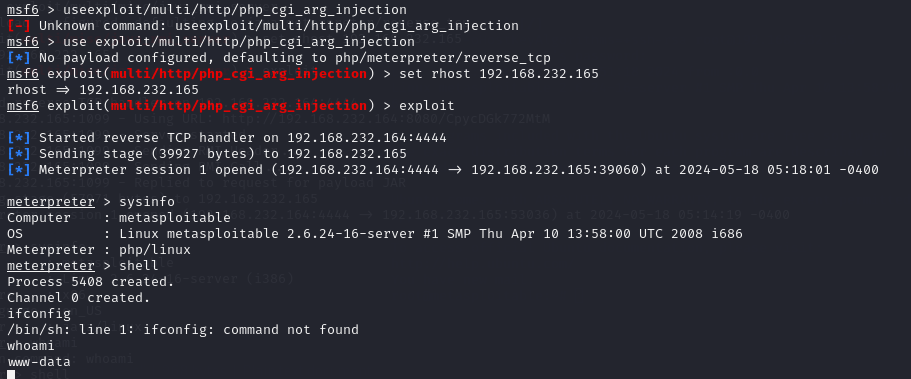
1. **Ingreslock后门漏洞（1524端口）:**

Ingreslock后门程序运行在1524端口，连接到1524端口就能直接获得root权限，经常用于入侵一个暴露的服务器。



1. **PHP CGI参数注入执行漏洞（80端口）:**

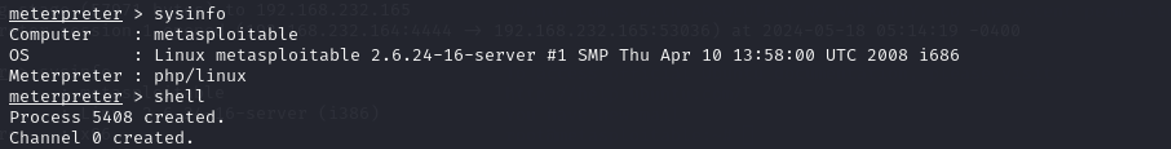
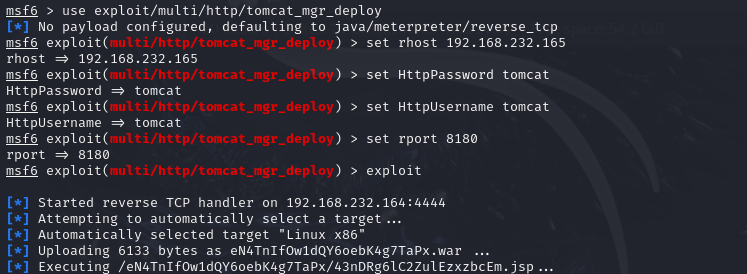
因为CGI脚本没有正确处理请求参数，而导致源代码泄露，允许远程攻击者在请求参数中插入执行命令。



1. **Tomcat管理台默认口令漏洞（8180端口）：**

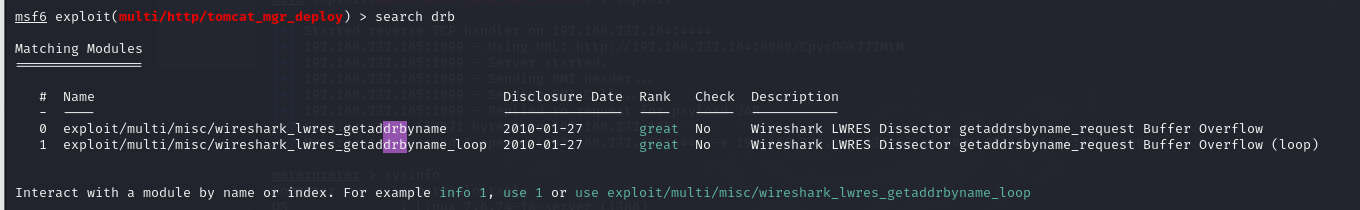
Tomcat管理台安装好后如果不及时修改默认管理账户并修改弱口令的话，有可能被黑客入侵，成功登陆者可以部署任意web应用,包括webshell。

在MSF下可以使用use multi/http/tomcat\_mgr\_deploy模块利用tomcat upload功能反弹shell。它的原理是上传一个war文件，在war文件执行对应的脚本，执行payload的内容：



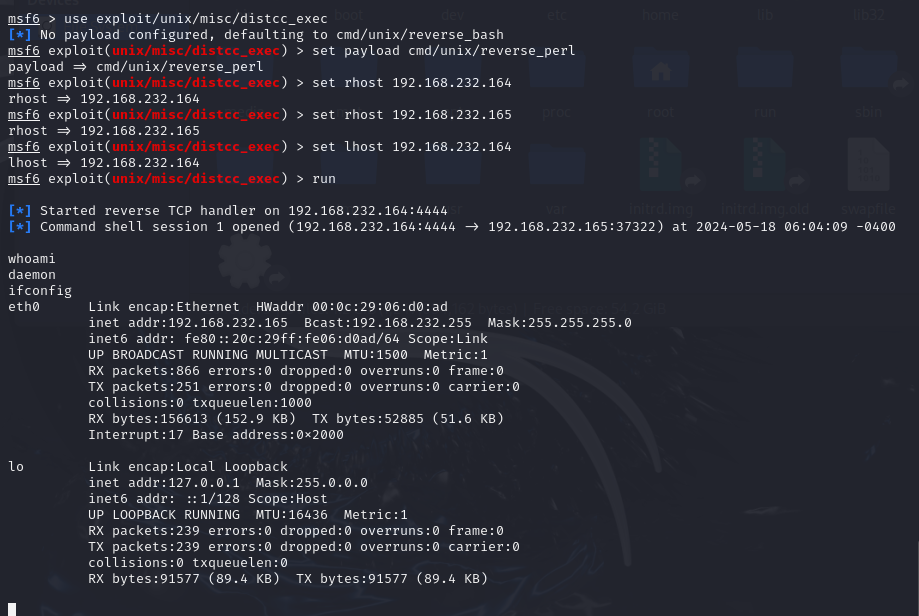
1. **Druby远程代码执行漏洞：**

当Druby配置不当时，其会被滥用执行命令，但是在MSF没有找对漏洞的对应渗透模块：



1. **Distcc后门漏洞（3623端口）：**

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，很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。



1. **实验思考及心得**

通过这次实验，我学习并掌握了Metasploit Framework的基本使用方法，了解了多种常见的网络安全漏洞及其利用手段，提高了实际操作技能和网络安全意识。