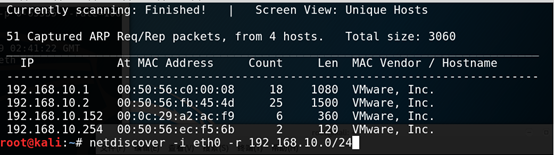
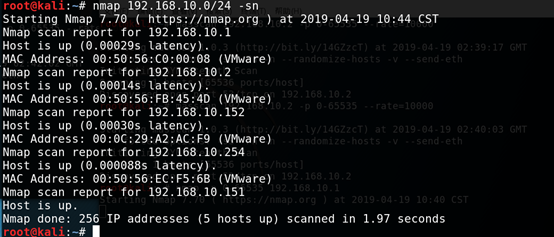
Lazysysadmin靶机

**一、主机发现(nmap/netdiscover)**

netdiscover -i eth0 -r 192.168.10.0/24



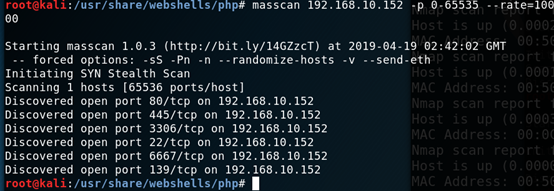
nmap 192.168.10.0/24 -sn



**二、端口扫描(masscan/nmap)**

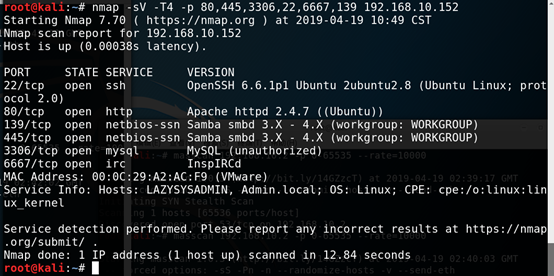
根据上面主机发现得到的主机,然后依次对每个主机进行快速端口扫描,分析得到自己要攻击的目标主机

masscan 192.168.10.152 -p 0-65535 --rate=10000



**三、识别端口上对应的服务**

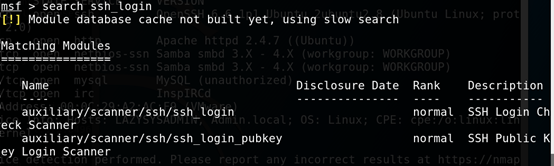
获取自己要攻击的目标主机上的端口之后,对开放的端口进行对应的服务识别



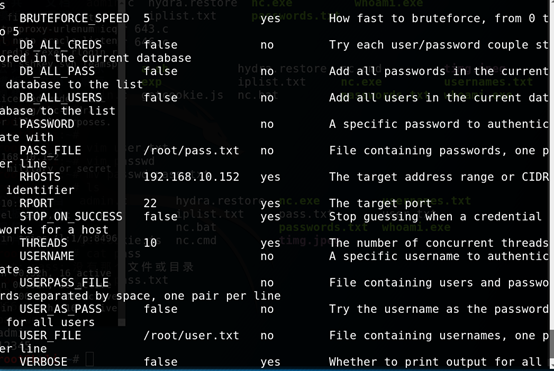
**四、发现服务对应的漏洞并利用**

1.首先从ssh服务入手,尝试暴力破解ssh

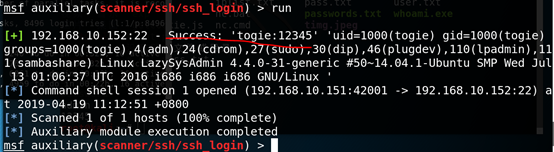
1.1使用msf的auxiliary/scanner/ssh/ssh\_login模块，爆破ssh



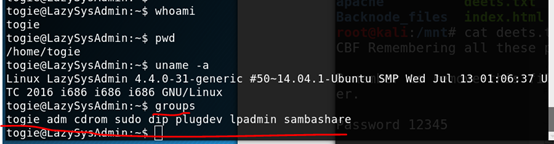
1.2设置参数



1.3开始攻击,下图可以看到成功爆破出用户名密码



尝试使用ssh服务登陆这个用户，成功登陆,查看用户所属组,此用户属于sudo组,具有管理员权限

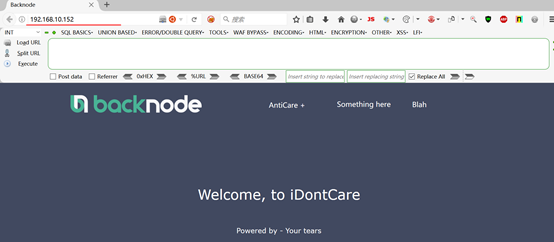


使用sudo su root切换到root账户

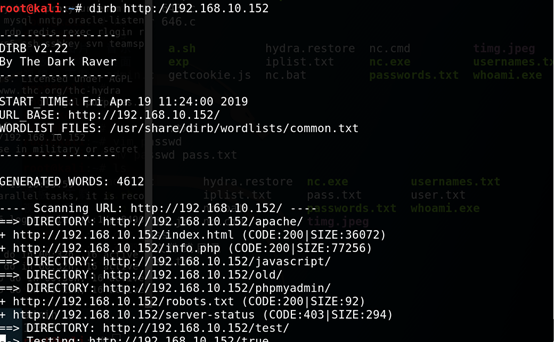


2. 目标开启apache服务，在网页中尝试web渗透

2.1通过浏览器访问http://192.168.10.152 , 分析整个网页,发现没有什么可以利用的

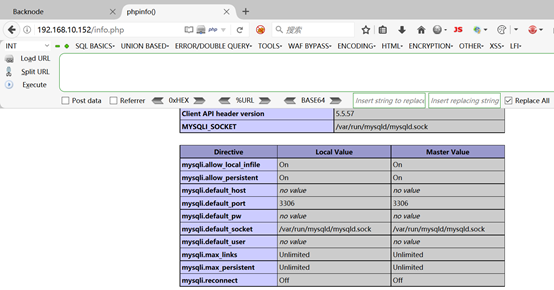


2.2利用目录扫描工具(dirb),扫描对应网站的目录

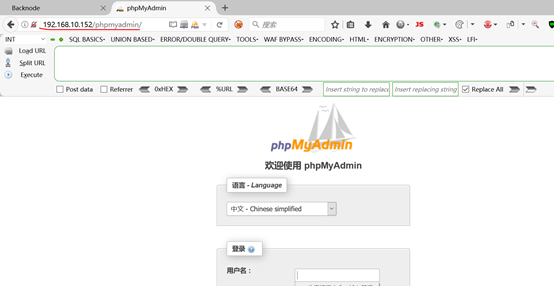


2.3对扫描出来的目录进行分析

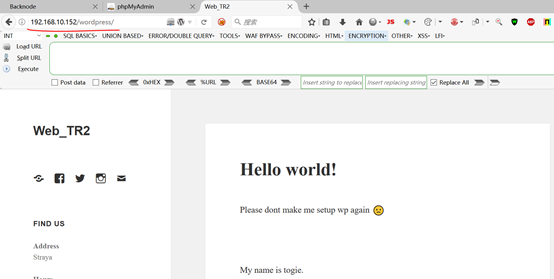
扫描出来info.php文件，浏览器访问,下图可以看到目标存在信息泄露漏洞



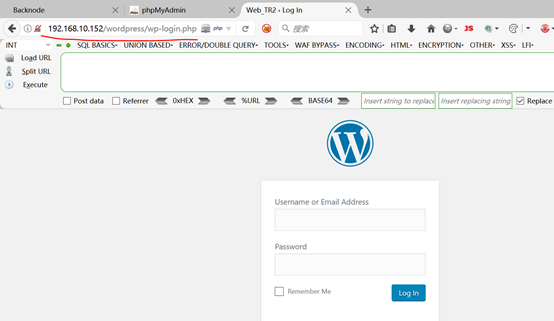
扫描出来/phpmyadmin/目录，浏览器访问,可以看到是mysql的后台登录界面,尝试弱口令或者暴力破解



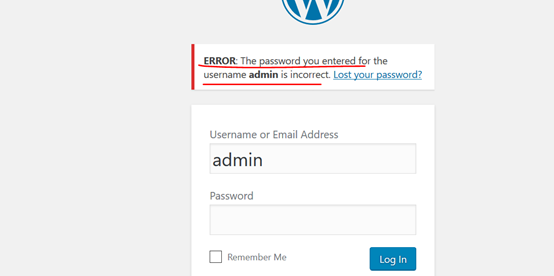
扫描发现wordpress ,浏览器访问，发现其中含有疑似用户名的信息



尝试登录wordpress的默认后台管理页面wp-login.php



尝试输入一些简单的弱口令,提示如下错误信息,发现用户名是admin,此处存在用户名名枚举漏洞,然后尝试暴力破解密码



使用wpscan扫描http://192.168.136.130/wordpress 看是否含有漏洞

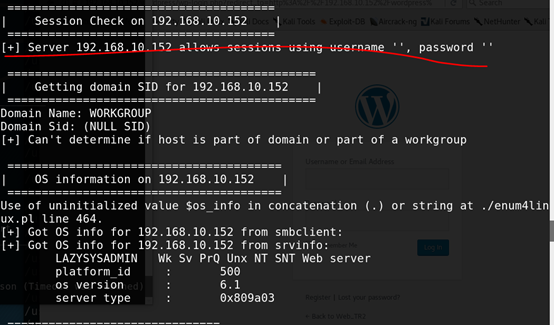
 Vp 只枚举有漏洞的插件，vt只枚举存在漏洞的主题，tt列举缩略图相关的文件

**3.尝试从samba服务发现漏洞**

使用enum4linux枚举运行samba的主机信息

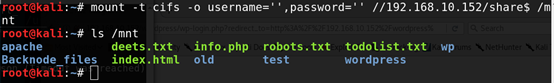
enum4linux 192.168.10.152

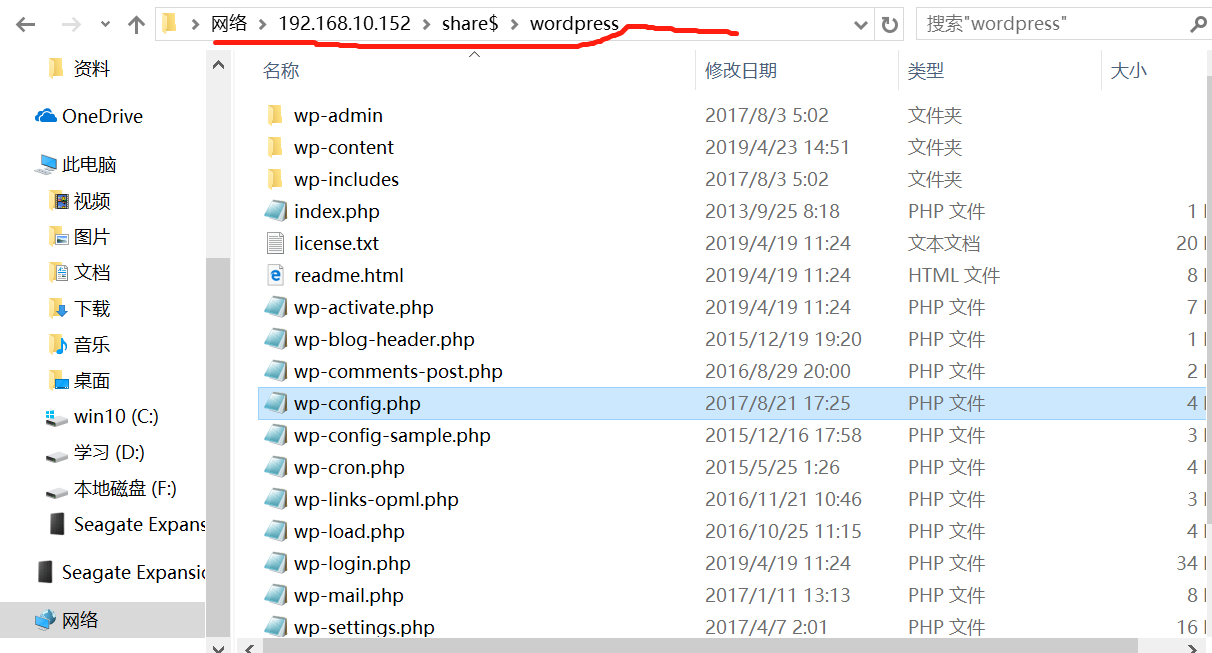
扫描完成后发现存在共享目录，允许空口令



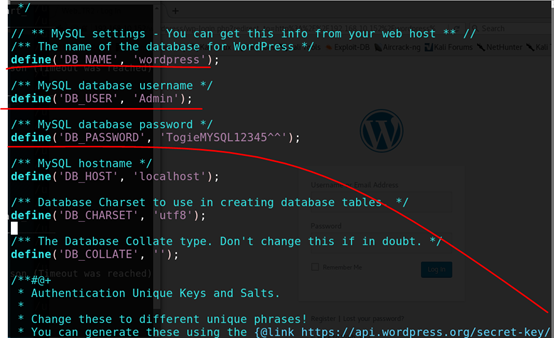
可以远程挂载，查看共享目录,发现共享的是网站的根目录

mount -t cifs -o username='',password='' //192.168.10.152/share$ /mnt



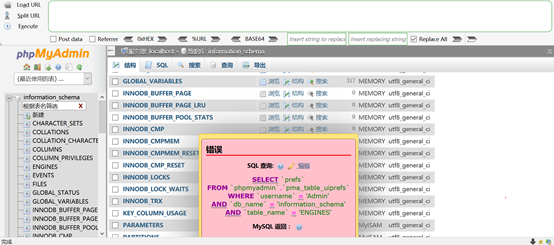
或者在windows访问共享　

Cd到wordpress目录,查看配置文件,可以看到wordpress后台的用户名以及密码



用得到用户名与密码尝试登录phpmyadmin,成功登录进去

尝试查看数据,发现此账户对数据库没有任何权限

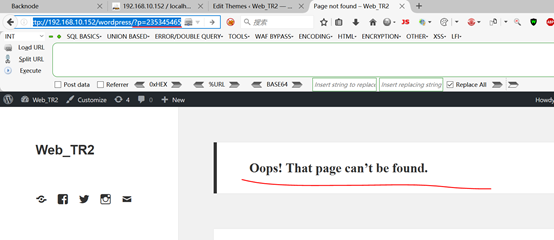


尝试用数据库的用户名密码登录wordpress后台,成功登录

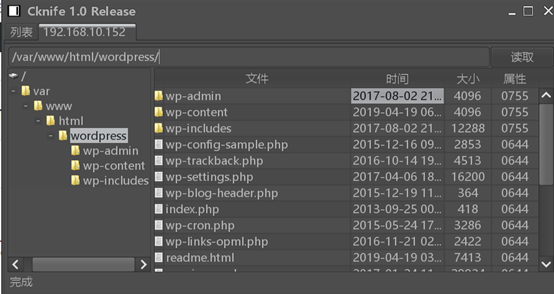
可以在一个404页面中添加一句话木马留后门,上传这个404页面



在浏览器访问一个不存在的页面,可以看到跳转到404页面,这时也就执行了插入其中的一句话木马



打开菜刀工具,连接url, 成功反弹shell



 总结：

1.信息收集

2.dirb目录爆破

3.ssh爆破

4.wpscan扫描wordpress漏洞

5.文件共享信息泄露

6.进入后台，Appearance页面404.php挂马，菜刀连接，反弹shell