g0rmint靶机实战

文章目录

[g0rmint靶机实战](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "g0rmint_0" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[1、主机发现](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "1_2" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[2、端口扫描](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "2_6" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[3、端口详细信息扫描](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "3_9" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[4、访问80端口--http服务](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "480http_11" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[5、getshell](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "5getshell_61" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[反弹shell方法一](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "shell_69" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

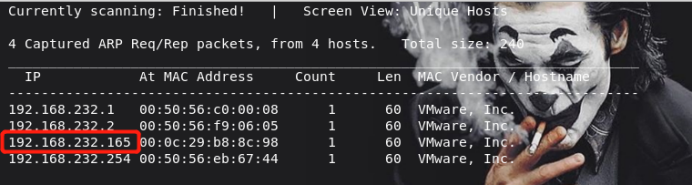
[反弹shell方法二](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "shell_77" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[6、提权](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "6_82" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

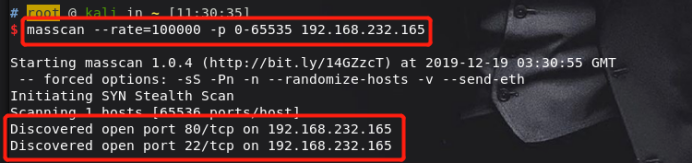
[方法一](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "_83" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

[方法二](https://blog.csdn.net/weixin_43870289/article/details/104115479" \l "_100" \t "https://blog.csdn.net/weixin_43870289/article/details/_self)

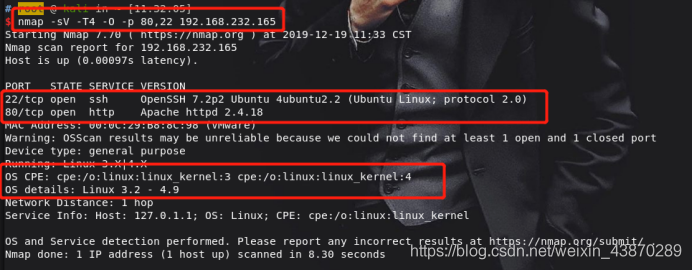
1、主机发现

arp-scan -l  
  
目标IP：192.168.232.165

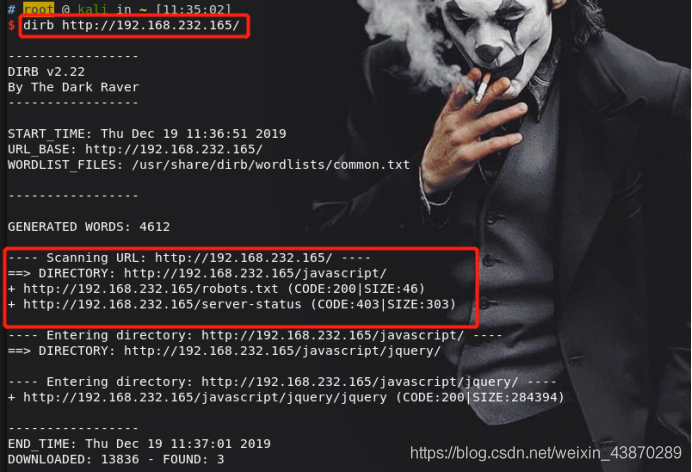
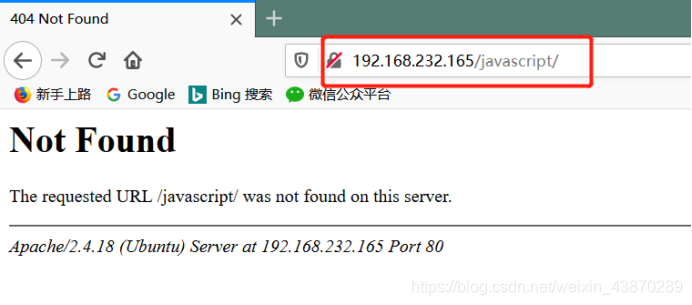
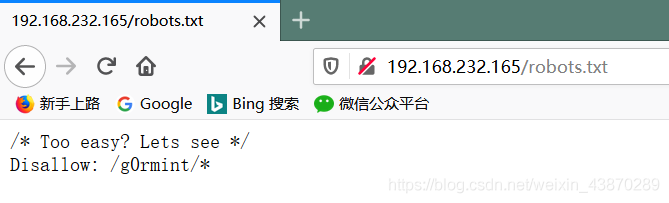
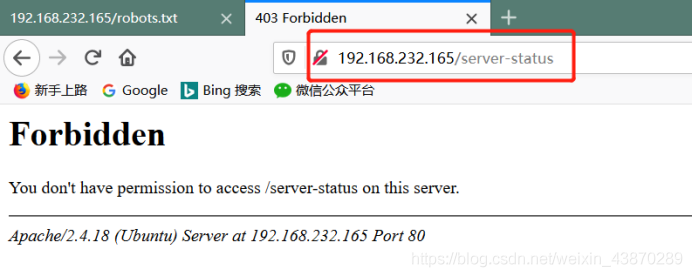
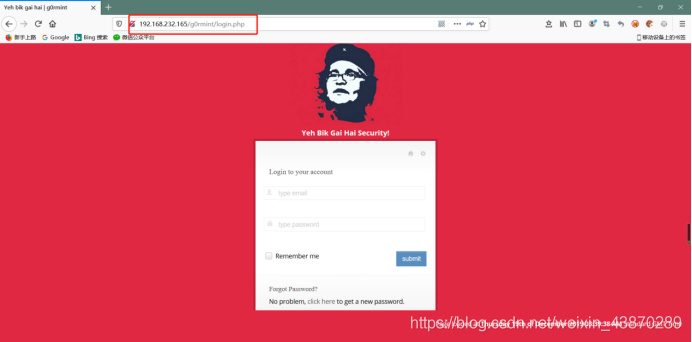
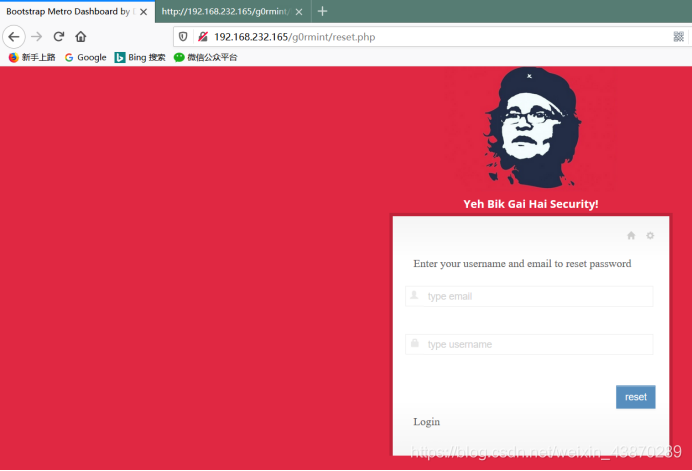
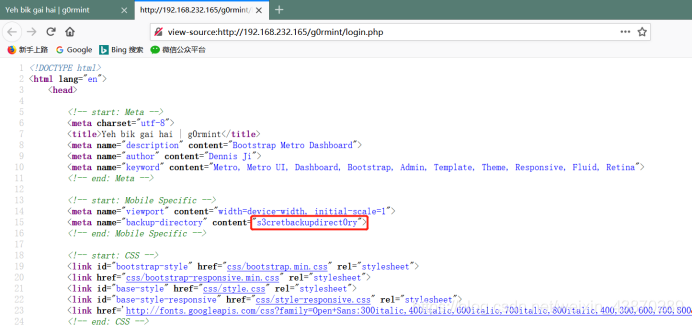
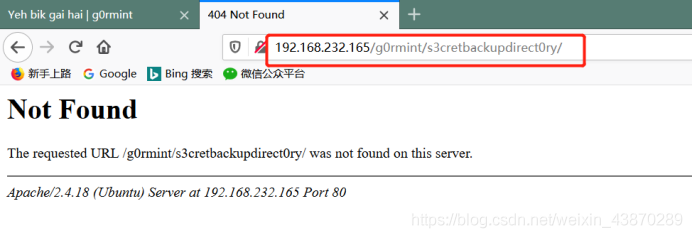
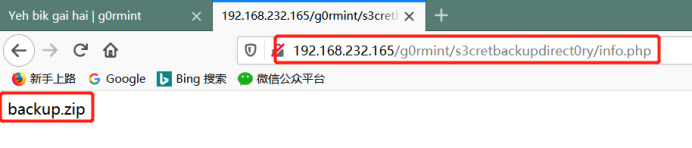
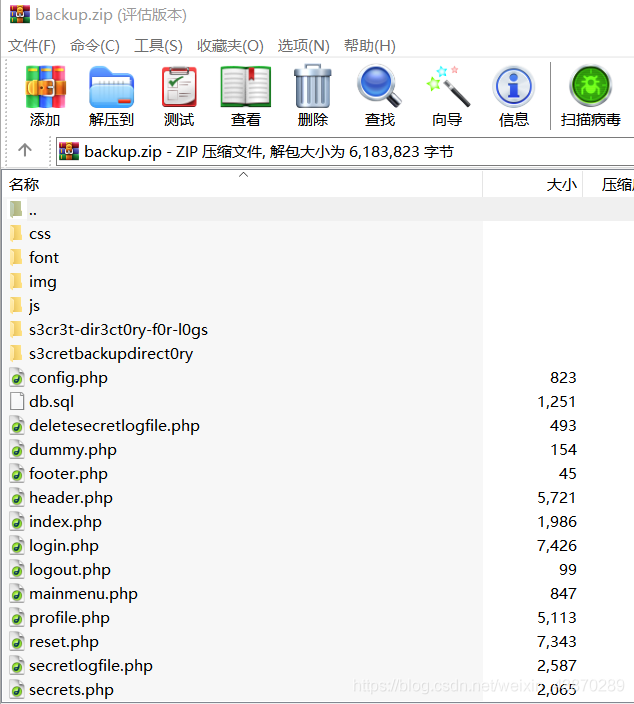
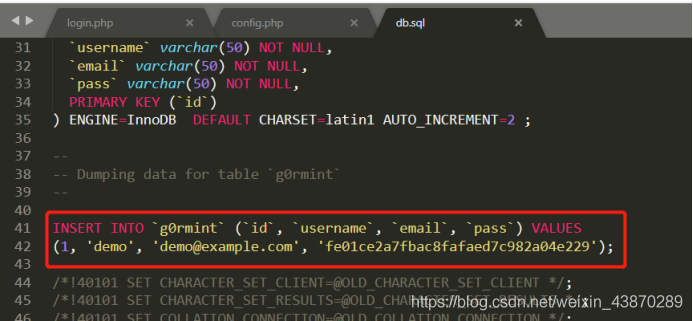
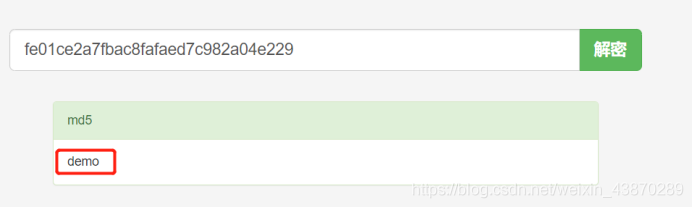
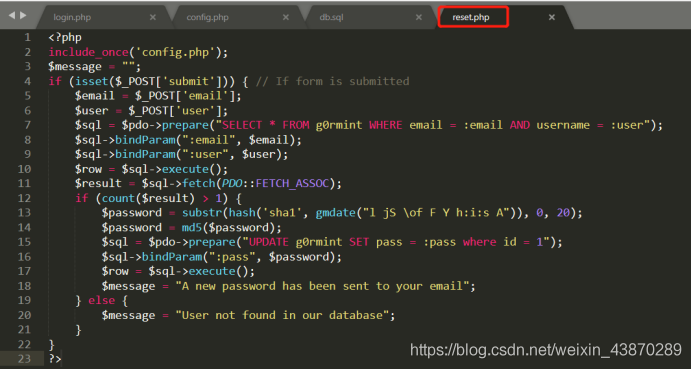
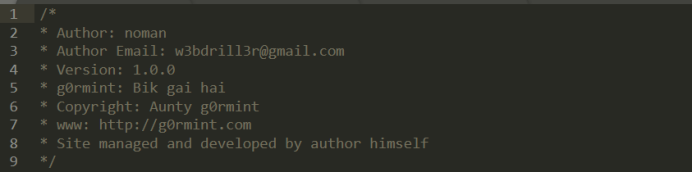
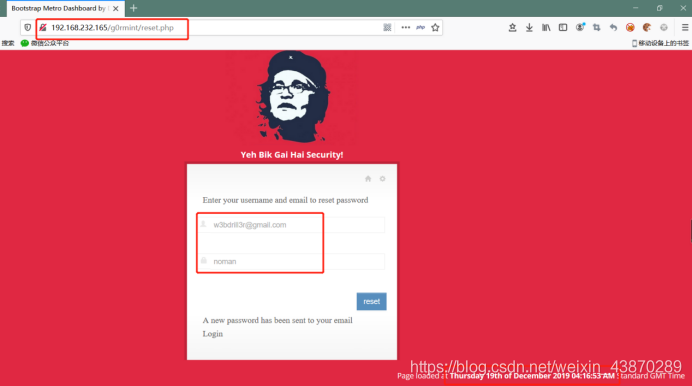
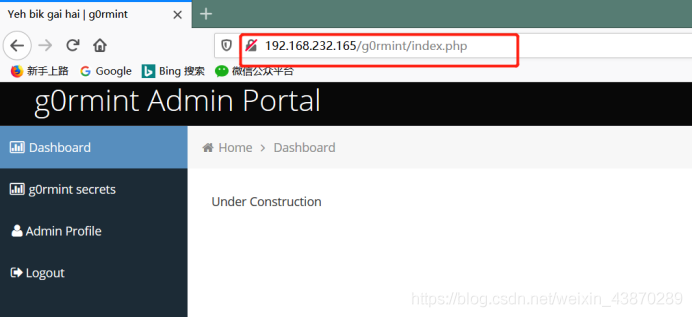
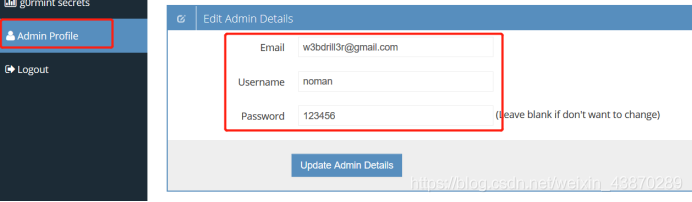
2、端口扫描

  
开放80、22端口

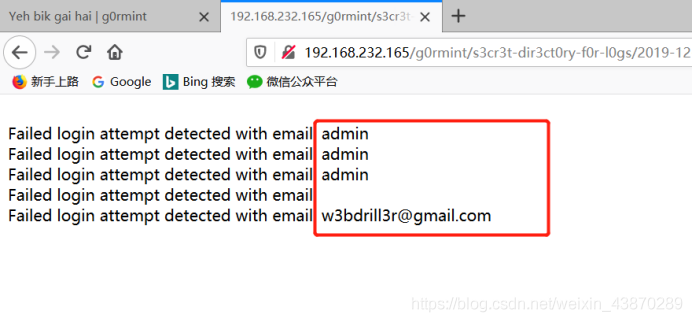
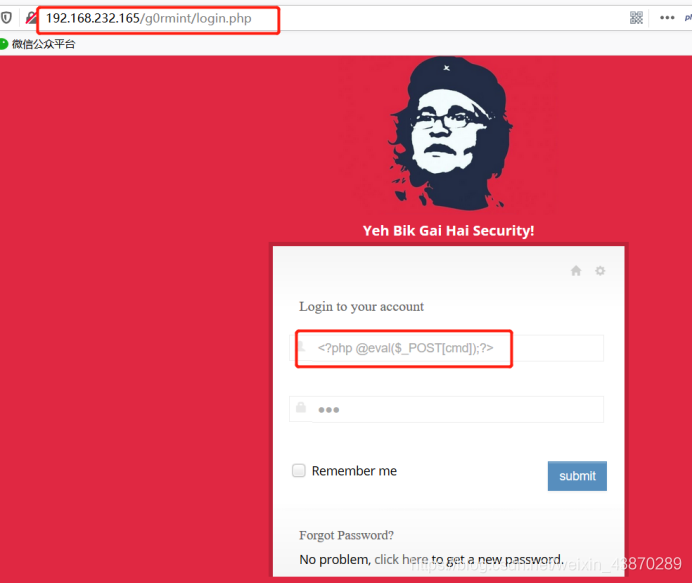
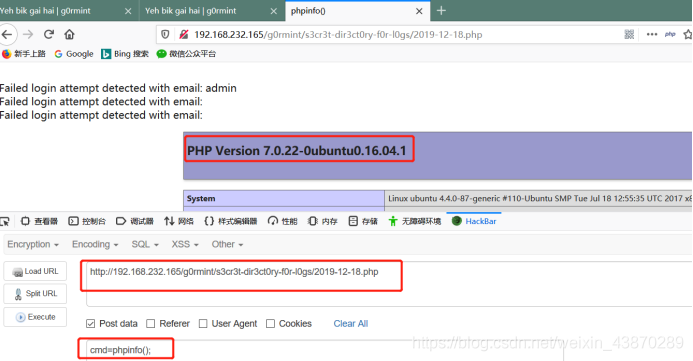
3、端口详细信息扫描



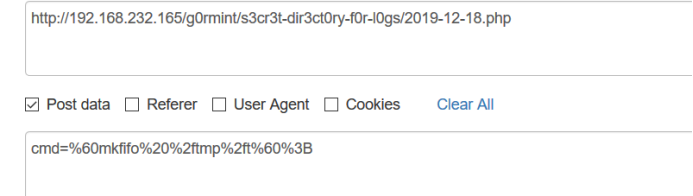
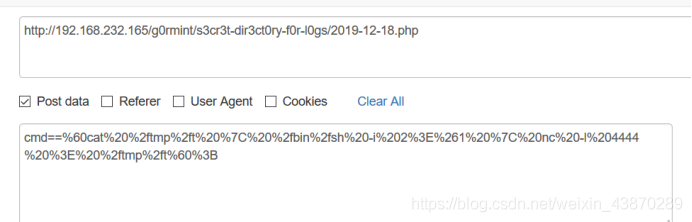
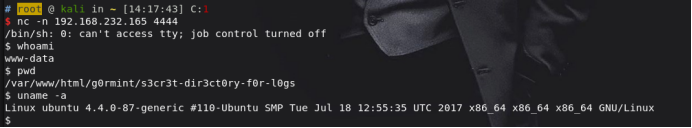
4、访问80端口–http服务

  
dirb扫一下其它目录  
  
依次访问：  
  
  
  
访问robots里面的地址：  
  
  
一个登录页面，先尝试弱口令：  
弱口令失败…  
查看源码：  
  
在html源代码中发现了一个不知道是什么东西的东西  
尝试访问一下：  
  
访问之后依旧是404，再用dirb爆一下目录：  
  
访问之：  
  
压缩包？下载看看：  
  
网站源码，下面涉及到代码审计：绝望…  
  
在login.php中可以看到，登录失败的时候会生成一个日志文件addlog($log, $reason);，看下这个addlog的代码  
  
发现登录失败日志存储在/s3cr3t-dir3ct0ry-f0r-l0gs目录下，格式为年月日.php，尝试访问一下：  
直接跳转到主页…  
继续看代码，在db.sql中可以看到一条插入的数据  
  
解密：  
  
尝试登录无果，看到文件中有一个重置密码的文件reset.php：  
  
可以看到，只需要知道一个存在的邮箱和用户名，就可以重置密码为一个时间值的哈希  
那就开始搜索邮箱和用户名：  
  
找到一个用户：noman（w3bdrill3r@gmail.com）  
尝试重置密码：  
  
成功重置，界面右下角也给出了对应的时间，遂能算出相应的哈希值  
获取重置后密码：  
  
算出重置后的密码为：02525a60b812a7a650b2  
登录：  
  
登录成功，先改个密码：  


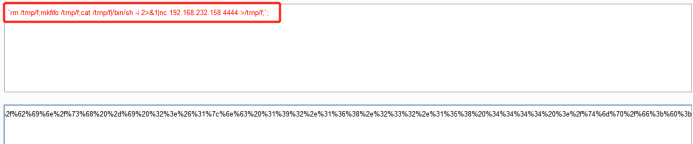
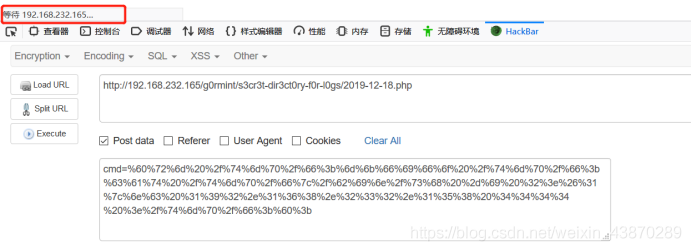
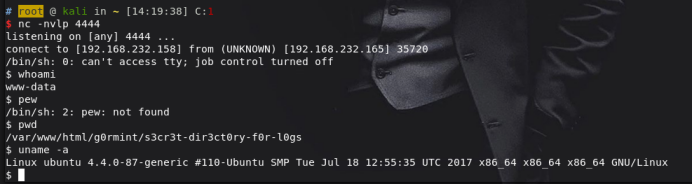
5、getshell

查看登录日志：  
  
登录失败日志记录着登录时的email信息，可以通过在登录的email处插入一句话木马，来获取shell：  
  
在访问日志文件：//利用hackbar提交post参数即可执行命令  
  
然后尝试反弹shell

反弹shell方法一

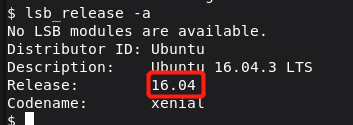
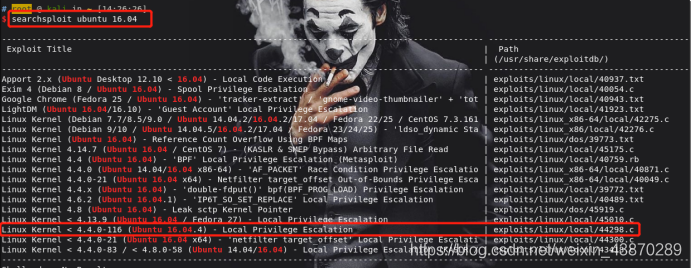
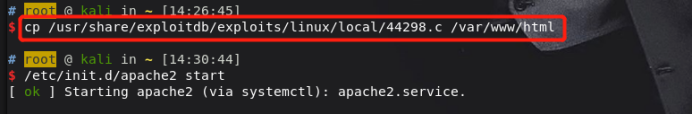
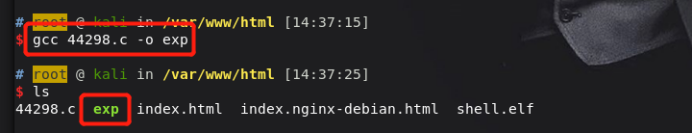
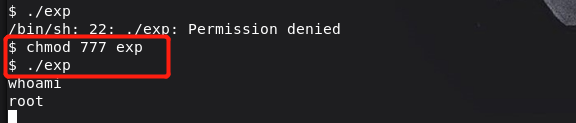
cmd=mkfifo /tmp/t;  
cmd=cat /tmp/t | /bin/sh -i 2>&1 | nc -l 4444 > /tmp/t  
进入阻塞状态，在kali中用nc连接即可  
  
  
在kali中用nc连接：  


反弹shell方法二

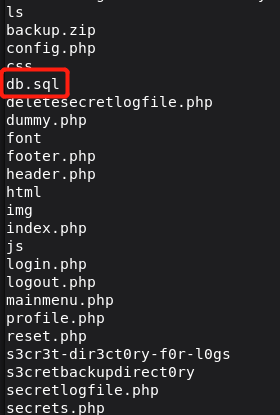
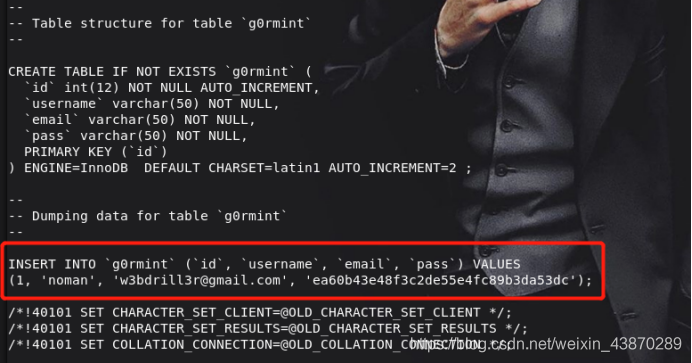
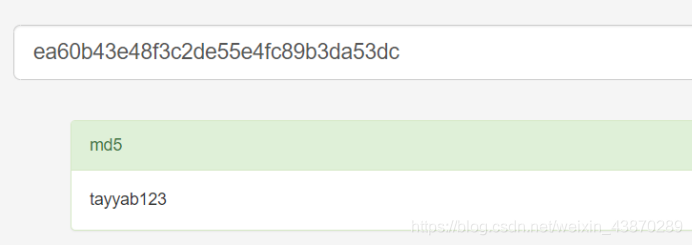
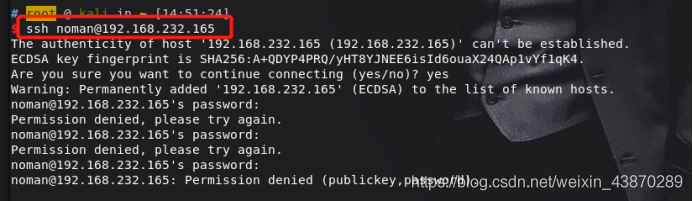
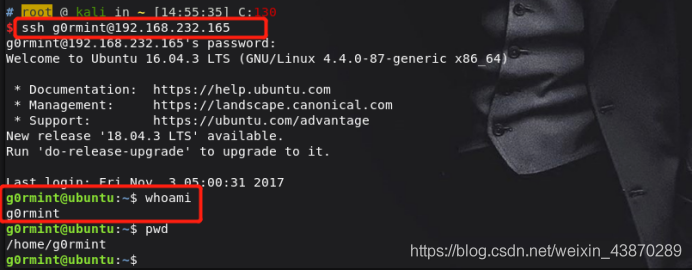
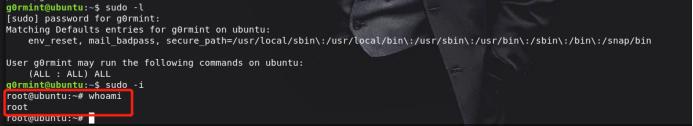
  
  
查看kali：//拿到shell  


6、提权

方法一

查看内核版本：  
  
kali搜索对应版本漏洞：  
  
挑44298.c来试试，将这个文件复制到/var/www/html目录下：//开启apache服务  
  
下载到靶机：  
  
编译：  
IMG_294  
没有安装gcc，尴尬…在kali编译好再上传吧：  
  
  
执行：//提示权限不够，赋权，再执行  
  
提权成功

方法二

在/var/www目录下又发现网站备份文件,解压发现db.sql  
IMG_298  
  
查看db.sql文件:  
  
发现用户noman以及密码:解密去  
  
拿到用户名：noman 密码：tayyab123  
因为这个靶机开放22端口，可以尝试去连接ssh  
  
又翻回去看了一下  
IMG_303  
//g0rmint 有点可疑，用这个试一下：  
  
成功登录  
然后用sudo -l 查看当前用户是否属于sudo组，接着使用sudo -i 直接获得管理员权限  
  
//全部命令都可以运行，nice