# Kioptrix Level 3

| | |
|---|---|
| Created | Feb 14, 2019 6:01 PM |
| Tags | Completed |
| Completed On | Feb 14, 2019 10:00 PM |

+ Add a Property

Add a comment...

## Finding machine IP address

```bash
sudo netdiscover -i eth1 -r 192.168.99.0/24
```

Bash

## Nmap scan

```bash
nmap -sV -sC -Pn -p- 192.168.99.100 -e eth1 -oN nmap
```

Bash

nmap 1.0KB

Nmap scan of all the 65535 ports of the system as only 2 ports popped up when scanned for first 1000 ports but even after such a thorough scan I was only able to get 2 ports open.

### Possible Network Attack Vectors

| Name | Status | Reason |
|---|---|---|
| 22 SSH | not-exploited | This server is never exploitable so I never even try to exploit these SSH services. |
| 80 HTTP | not-exploited | There was no exploit available for Apache 2.2.8 which directly got me a shell in the system. So I went with other paths for exploiting this machine. |

+ New

COUNT 2

## GoBuster Directory scanning for attack vectors

```bash
gobuster -e -t 100 -u http://kioptrix3.com/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

Bash

gobuster 1.0KB

GoBuster Directory scan with the small directory listings. Found many possible exploit vectors.

### Possible WebApp Attack Vectors

| Name | Status | Reason |
|---|---|---|
| /index.php?page=index.php | exploited | Got a lotus CMS exploit which got me the meterpreter session. |
| /phpmyadmin | | |

+ New

COUNT 2

## LotusCMS `eval() page=value param` exploit

Exploit: `exploits/php/remote/18565.rb`

Metasploit Module: `exploit/multi/http/lcms_php_exec`

Used netcat reverse shell along with python pty shell to get a semi-stable tty shell on my machine. `python -c 'import pty; pty.spawn("/bin/bash")'`

Ran `LinEnum.sh` to get some more information about the machine, after getting some information I tried running the following exploits but to no avail, I got nothing.

Got me shell as `www-data` Tried several exploits none of them worked, all the exploits are listed below.

- Bash Exploit: `exploits/multiple/local/11651.sh`
- Kernel DirtyCow: `exploits/linux/local/40611.c, exploits/linux/local/40616.c, exploits/linux/local/40838.c`
- Bash Exploit: `exploits/multiple/local/7129.sh`
- Kernel VMSplice Exploit: `exploits/linux/local/5093.c, exploits/linux/local/5092.c`

Tried searching through the files to get some login information

Ran `grep -p 'password' -r ./` to search for some password parameters, came across some interesting mysql parameters values with `gallarific_mysql` this phrase, ran grep again with this and came across MySQL username, password, and production database in use.

```bash
Username: root Password: fuckeyou Database: gallery
```

Bash

Log-into the MySQL server and enumerated to get the following data.

```
mysql> select * from dev_accounts; [19/1647] select * from
dev_accounts; +----+------------+--------------------------
--------+ | id | username | password | +----+------------+-
---------------------------------+ | 1 | dreg |
0d3eccfb887aabd50f243b3f155c0f85 | | 2 | loneferret |
5badcaf789d3d1d09794d8f021f40f0e | +----+------------+-----
-----------------------------+ 2 rows in set (0.01 sec)
mysql> select * from gallarific_users; select * from
gallarific_users; +--------+----------+----------+---------
--+-----------+----------+-------+------------+---------+--
-----------+-------+----------+ | userid | username |
password | usertype | firstname | lastname | email |
datejoined | website | issuperuser | photo | joincode | +--
------+----------+----------+-----------+-----------+------
----+-------+------------+---------+-------------+-------+-
---------+ | 1 | admin | n0t7t1k4 | superuser | Super |
User | | 1302628616 | | 1 | | | +--------+----------+------
----+-----------+-----------+----------+-------+-----------
-+---------+-------------+-------+----------+ 1 row in set
(0.04 sec)
```

SQL

The dev accounts noted above are the users in the system as evident from the home folder. The other account is to login to the admin page for the Gallery application.

The passwords were store as MD5 hashes and the mapping came out to be `dreg:Mast3r` and `loneferret:starwars`

Using the credentials above I SSHed into the server with loneferret's account and tried running `sudo ht` but the terminal colours were not correct so changed my terminal colours to some suitable value for `sudo ht` to run correctly. I used `export TERM=xterm` for the `ht` to run correctly.

Using the editor I changed the `/etc/sudoers` file and granted `loneferret` all the privileges and then `sudo bash` to get root and got the flag from `/root`

> Learning: Sometime boxes are not about running the exploits, try information gaining as well and leverage it to do some manual stuff. Running exploits is fun but this box is something else. Completely takes a different track. It was fun.